Universidade Federal de Uberlândia
Universidade Aberta do Brasil
Centro de Educação a Distância

Introdução à Teoria dos Números

Ana Maria Amarillo Bertone

Bertone, Ana Maria Amarillo
Introdução à Teoria dos Números/ Ana Maria Amarillo Bertone.

Uberlândia, MG : UFU, 2014, 202 p.

Licenciatura em Matemática

1. Introdução à Teoria dos Números

Edição
Centro de Educação a Distância
Comissão Editorial-CEAD/UFU

Diagramação
Ana Maria Amarillo Bertone

PRESIDENTE DA REPÚBLICA
Dilma Vana Rousseff

MINISTRO DA EDUCAÇÃO
Aloizio Mercadante

UNIVERSIDADE ABERTA DO BRASIL
DIRETORIA DE EDUCAÇÃO A DISTÂNCIA/CAPES
João Carlos Teatini de Souza Clímaco

UNIVERSIDADE FEDERAL DE UBERLÂNDIA - UFU
REITOR
Elmiro Santos Resende

VICE-REITOR
Eduardo Nunes Guimarães

CENTRO DE EDUCAÇÃO A DISTÂNCIA
DIRETORA E REPRESENTANTE UAB/UFU
Maria Teresa Menezes Freitas

SUPLENTE UAB/UFU
José Benedito de Almeida Júnior

FACULDADE DE MATEMÁTICA -FAMAT - UFU
DIRETOR
Luís Antônio Benedetti

COORDENADOR DO CURSO DE LICENCIATURA EM MATEMÁTICA - PARFOR
Douglas Marin

PROFESSOR
Ana Maria Amarillo Bertone

ASSESSORA DA DIRETORIA
Sarah Mendonça de Araújo

EQUIPE MULTIDISCIPLINAR
Danilo Adrian Marques
Alberto Dumont Aves Oliveira
Dirceu Nogueira de Sales Duarte Jr.
Gustavo Bruno do Vale
João Victor da Silva Alves
Otaviano Ferreira Guimarães

Sumário

Informações úteis

Prezado(a) aluno,

Lembramos novamente como no módulo I que no texto básico você encontrará alguns " ícones" que lhe ajudará a identificar as atividades. Fique atento ao significado de cada um deles, isso facilitará a sua leitura e seus estudos.

Lembramos também alguns termos ou conceitos são destacados ao longo do texto básico em um quadro de borda vermelho, em negrito e em letras de cor azul seguido pelo ícone do AVA, da forma que aparece esta palavra **número natural**  . Fique atento, pois esta é parte de umas das atividades do seu curso: você irá construir, como no módulo I, junto com seus colegas, um glossário que irá conter esses termos ou conceitos. Procure também associar ao termo uma imagem que esclareça seu sentido ou permita uma melhor fixação e visualização da ideia. É a atividade de *Glossário*.

Desejamos ao caro aluno(a) um ótimo segundo módulo, torçendo para que atinja com sucesso os seus objetivos.

Estou à disposição em https://sites.google.com/site/anamariaufumat/Home

Grande abraço,

Ana Maria

Sobre a autora

Ana Maria Amarillo Bertone – Licenciada em Matemática pelo Instituto de Professores Artigas (IPA) da cidade de Montevidéu, Uruguay, de onde é natural. Mestre em Matemática Aplicada pela Universidade Federal do Rio de Janeiro, RJ. Possui doutorado em Matemática pela Universidade de Brasília (UnB). Durante nove anos dedicou-se ao ensino médio, de onde surge a paixão pelo desenvolvimentos de métodos didáticos de ensino com foco na tecnologia. Desde 1991 até 2003 foi professora da Universidade Federal da Paraíba, João Pessoa, PB, onde desenvolveu trabalhos de pesquisa em Equações Diferenciais Parciais (EDP) e colaborou para a fundação do primeiro mestrado do estado da Paraíba. Fez pós-doutorado na Universidade de Rutgers – New Jersey, no ano de 1999 e na Universidade de Washington, Seattle – WA, no ano de 2003, aonde residiu por vários anos. De volta ao Brasil, em 2008, exerce o cargo professora na Faculdade de Matemática da UFU, participando de projetos de pesquisa na área de EDP com parâmetros fuzzy. Visitou em 2012 a Universidad Pedagógica Nacional Francisco Morazán, Honduras, como professor visitante voluntário da União Internacional de Matemática (IMU), para ministrar cursos de apóio ao curso de Licenciatura da mesma universidade. Presidente do Instituto GeoGebra de Uberlândia, tem participado de projetos de extensão para professores da rede pública municipal e para aprimoramente discente, como foco em material didático envolvendo softwares e tecnologia.

Sobre o curso

A teoria dos números é uma área específica da matemática que estuda as propriedades dos números inteiros, tais como a divisibilidade, números primos, tendo entre os resultados mais destacados o Teorema Fundamental da Aritmética. Com esses objetivos específicos, esta área é das mais antigas da matemática, junto com a Geometria Euclidiana. Os quatro volumes de *Os Elementos* de Euclides foram inteiramente dedicados à teoria dos números entendida como a clássica aritmética.

O grande matemático Carl Friedrich Gauss, de cujo trabalho iremos encontrar, ao longo do texto básico, alguns resultados, escreveu uma frase que salienta a importância desta área da matemática:

> A matemática é a rainha das ciências e a aritmética, a rainha da matemática.[a]
>
> [a]Traduzido do inglês: *"Mathematics is the queen of sciences and arithmetic the queen of mathematics."*

Entre alguns exemplos importantes de *problemas em aberto*, apresentamos aqueles que podem fazer famoso a algum pequisador, estudante o simplesmente a um(a) amante da matemática (quem sabe um de vocês!)

Muitos deles são relacionados com *números primos*, que são aqueles números que têm como únicos divisores eles mesmos e a unidade.

1. (*Conjectura de Goldbach*) Todo número natural $n > 2$ é soma de dois números primos.
2. Será que existem infinitos números primos da forma $n^2 + 1$?
3. Será que existem infinitos números primos da forma $2^n - 1$? Estes números primos são chamados de *Mersenne*.
4. Será que existem infinitos números primos da forma $2^{2^n} + 1$? Estes números primos são chamados de *Fermat*.

Em nosso curso iremos conhecer algumas das técnicas que os matemáticos usam para desvendar estes mistérios.

Além do estudo da matéria básica da teoria dos números, faremos considerações teóricas sobre as estruturas dos conjuntos numéricos dos números racionais e dos números reais. Vamos comparar a estrutura de todos estes conjuntos, o que eles têm em comum ou o que os distingue dos demais.

A presente disciplina está dividida em quatro módulos:

- ▷ O conjunto dos números Inteiros;
- ▷ Congruência;
- ▷ O conjunto dos números racionais;
- ▷ O conjunto dos números reais.

A duração de cada módulo é de quinze dias. O texto básico da disciplina é contemplado com exercícios estrategicamente posicionados, de tal forma que o conteúdo previamente estudado fique bem assimilado em seus conceitos mais básicos.

O texto básico da disciplina é contemplado com exemplos e exercícios propostos sob a forma de **desafio** que você encontrará estrategicamente posicionados. Estes desafios incluem a resposta que está no final de cada módulo. Para acessar a resposta você vai clicar um hiperlink que o levará de ida e volta para o final de módulo ou para a página do desafio. Para maior eficiência desta metodologia, recomendamos ao prezado aluno tentar o desafio antes de clicar o hiperlink que o conduz à resposta.

Quanto à metodologia, o curso seguirá com a seguinte base: estudo da teoria do livro texto, com o treino através dos exercícios nele contidos, resolução do *Caderno de Exercícios*, onde se encontram os exercícios a serem entregues e outros para que o aluno se pratique. Atividades que serão passadas para os alunos dentro do período de vigência de cada módulo, e que farão parte do processo de avaliação, assim como as provas presenciais.

Quanto ao sistema de avaliação, serão distribuídos 100 pontos, sendo 60 pontos de provas escritas em modo presencial e 40 pontos das atividades passadas pelo Ambiente Virtual de Aprendizagem (AVA).

Quanto ao cronograma, descrito mais adiante, as 75 horas do curso são distribuídas nos módulos de acordo com o número de semanas, considerando 4 horas de atividades de estudo da teoria por semana, sendo necessário considerar para cada hora de estudo em teoria pelo menos uma hora de estudo através de exercícios. Esse esquema tem por finalidade assegurar um treino mínimo nos módulos.

Desejamos ao caro aluno um ótimo curso, torçendo para que atinja com sucesso os objetivos da disciplina.

Estou à disposição em https://sites.google.com/site/anamariaufumat/Home

Grande abraço,

Ana Maria

Agenda

Módulo Tópico Período	Atividade	Desenvolvimento do Conteúdo
Módulo III **OS NÚMEROS INTEIROS** **Primeira Quinzena**	**Atividade 1:** Assistir à vídeo aula introdutória.	Para auxiliar ao aluno no entendimento dos assuntos tratados neste Módulo, é disponibilizada uma vídeo aula gravada pela autora.
	Atividade 2: Leitura do Texto Básico	Neste módulo o aluno aprenderá a fazer demonstrações pelo método de indução. Aplicará seus conhecimentos sobre divisores e múltiplos de números naturais, com uma nova base teórica, que explica os mecanismos utilizados na prática. Aprenderá novos mecanismos desses cálculos, como os de achar máximo divisor comum de dois números inteiros.
	Atividade 3: Webconferências	Para ampliar as informações sobre os assuntos estudado neste Módulo, serão realizadas duas webconferências.
	Atividade 4: Testando seus conhecimentos: etapas I e II.	O Caderno de Exercícios tem como objetivo que o aluno se pratique bastante antes de resolver os exercícios obrigatórios. Estes são os exercícios do mesmo caderno que estão enquadrados em cor verde ou amarela, constituindo as duas etapas da atividade 4. É uma atividade de avaliação.
	Atividade 5: Glossário do Módulo I	Após a leitura do Texto Básico, o aluno irá definir os conceitos que foram salientados da forma seguinte: **número natural**  . Atividade de avaliação.
	Atividade 6: Fórum	Atividade desenvolvida no Moodle para discussão do Caderno de Exercícios (atividade avaliativa) e de dúvidas (não avaliativa)
	Atividade 7: Leitura Complementar	Esta atividade é para o aluno enriquecer seus conhecimentos, descobrir aplicações dos tópicos propostos ou simplesmente um bom material de leitura.

Módulo Tópico Período	Atividade	Desenvolvimento do Conteúdo
Módulo III **C O N G R U Ê N C I A S** **Primeira Quinzena**	**Atividade 1:** Assistir à vídeo aula introdutória.	Para auxiliar ao aluno no entendimento dos assuntos tratados neste Módulo, é disponibilizada uma vídeo aula gravada pela autora.
	Atividade 2: Leitura do Texto Básico	Neste módulo o aluno vai conhecer o tópico de congruência, uns dos mais importantes da Teoria dos Números, pelas suas aplicações nas ciências e tecnologia. Aprenderá a resolver equações diofantinas e de congruência linear. Aplicará a congruência para resolver problemas de divisibilidade não vistos anteriormente.
	Atividade 3: Webconferências	Para ampliar as informações sobre os assuntos estudado neste Módulo, serão realizadas duas webconferências.
	Atividade 4: Testando seus conhecimentos: etapas I e II.	O Caderno de Exercícios tem como objetivo que o aluno se pratique bastante antes de resolver os exercícios obrigatórios. Estes são os exercícios do mesmo caderno que estão enquadrados em cor verde ou amarela, constituindo as duas etapas da atividade 4. É uma atividade de avaliação.
	Atividade 5: Glossário do Módulo I	Após a leitura do Texto Básico, o aluno irá definir os conceitos que foram salientados da forma seguinte: **número natural**  . Atividade de avaliação.
	Atividade 6: Fórum	Atividade desenvolvida no Moodle para discussão do Caderno de Exercícios (atividade avaliativa) e de dúvidas (não avaliativa)
	Atividade 7: Leitura Complementar	Esta atividade é para o aluno enriquecer seus conhecimentos, descobrir aplicações dos tópicos propostos ou simplesmente um bom material de leitura.

Módulo Tópico Período	Atividade	Desenvolvimento do Conteúdo
Módulo III **OS NÚMEROS RACIONAIS** **Primeira Quinzena**	**Atividade 1:** Assistir à vídeo aula introdutória.	Para auxiliar ao aluno no entendimento dos assuntos tratados neste Módulo, é disponibilizada uma vídeo aula gravada pela autora.
	Atividade 2: Leitura do Texto Básico	Neste módulo você verá a construção dos números racionais, a sua representação decimal, dando uma estrutura teórica a mecanismos que você muito bem conhece e ensina ou ensinará no futuro. Além de estudar o conceito de enumerabilidade, demosntrando que o conjunto dos números racionais tem o mesmo cardinal que o conjunto dos números naturais.
	Atividade 3: Webconferências	Para ampliar as informações sobre os assuntos estudado neste Módulo, serão realizadas duas webconferências.
	Atividade 4: Testando seus conhecimentos: etapas I e II.	O Caderno de Exercícios tem como objetivo que o aluno se pratique bastante antes de resolver os exercícios obrigatórios. Estes são os exercícios do mesmo caderno que estão enquadrados em cor verde ou amarela, constituindo as duas etapas da atividade 4. É uma atividade de avaliação.
	Atividade 5: Glossário do Módulo I	Após a leitura do Texto Básico, o aluno irá definir os conceitos que foram salientados da forma seguinte: **número natural**  . Atividade de avaliação.
	Atividade 6: Fórum	Atividade desenvolvida no Moodle para discussão do Caderno de Exercícios (atividade avaliativa) e de dúvidas (não avaliativa)
	Atividade 7: Leitura Complementar	Esta atividade é para o aluno enriquecer seus conhecimentos, descobrir aplicações dos tópicos propostos ou simplesmente um bom material de leitura.

Módulo Tópico Período	Atividade	Desenvolvimento do Conteúdo
Módulo III **OS NÚMEROS REAIS** **Terceira Quinzena**	**Atividade 1:** Assistir à vídeo aula introdutória.	Para auxiliar ao aluno no entendimento dos assuntos tratados neste Módulo, é disponibilizada uma vídeo aula gravada pela autora.
	Atividade 2: Leitura do Texto Básico	Neste módulo o aluno verá a construção dos números reais pela sua representação decimal, a partir da estrutura dos números racionais na mesma representação. Estudaremos os números irracionais, sua aritmética, e as duas classes importantes de números irracionais: os números algébricos e transcendentes.
	Atividade 3: Webconferências	Para ampliar as informações sobre os assuntos estudado neste Módulo, serão realizadas duas webconferências.
	Atividade 4: Testando seus conhecimentos: etapas I e II.	O Caderno de Exercícios tem como objetivo que o aluno se pratique bastante antes de resolver os exercícios obrigatórios. Estes são os exercícios do mesmo caderno que estão enquadrados em cor verde ou amarela, constituindo as duas etapas da atividade 4. É uma atividade de avaliação.
	Atividade 5: Glossário do Módulo I	Após a leitura do Texto Básico, o aluno irá definir os conceitos que foram salientados da forma seguinte: **número natural**  . Atividade de avaliação.
	Atividade 6: Fórum	Atividade desenvolvida no Moodle para discussão do Caderno de Exercícios (atividade avaliativa) e de dúvidas (não avaliativa)
	Atividade 7: Leitura Complementar	Esta atividade é para o aluno enriquecer seus conhecimentos, descobrir aplicações dos tópicos propostos ou simplesmente um bom material de leitura.

Anotações

Módulo 1
O conjunto dos Inteiros

No término do módulo I, o aluno estará familiarizado como os seguintes conceitos:

- O conjunto dos números naturais;
- O conjunto dos números inteiros;
- Múltiplos e divisores;
- O algoritmo da divisão;
- Máximo divisor comum e mínimo múltiplo comum;
- O algoritmo de Euclides;
- Números primos.

1.1 Os Números Naturais

O que há em comum entre um saco com 20 maças e uma lista de supermercado com 20 ítens?

A resposta “trivial” para isso é o **número** de elementos desses objetos (saco de maçãs e lista de supermercado). Mas então,o quais dos **conceitos de número** é que define uma qualidade em comum desses dois conjuntos tão diferentes?

É o conceito de **número natural** 

.

Do ponto de vista teórico, o **modelo matemático** 

que tem as características de um modelo de contagem é o do **conjunto dos números naturais**.

Uma lista ordenada desses números foi o princípio da teoria de todos os números. De acordo com Elon Lages Lima:

"Comparar conjuntos de objetos com essa escala abstrata ideal é o processo que torna mais precisa a noção de quantidade; esse processo (a contagem) pressupõe portanto o conhecimento da sequência numérica."

Imaginemos por um instante que não conhecemos esta lista de números mas sabemos que gostaríamos que os números naturais fossem aqueles da contagem de objetos. Então,

Quais seriam as caraterísticas principais que fazem o conjunto dos números naturais o conjunto modelo para a contagem?

Foi o matemático italiano Giussepe Peano (1858-1932) que introduziu pela primeira vez os **axiomas** que caraterizam os números naturais e que levam seu nome: os axiomas de Peano.

Axiomas de Peano

1. Todo número natural n possui um único sucessor que é um número natural.
2. Se dois números naturais têm o mesmo sucessor então são iguais.
3. No conjunto dos números naturais existe um único número, denotado por 1, que não é sucessor de nenhum outro.
4. Seja um subconjunto A de números naturais que verifica
   - $1 \in A$;
   - dado um número natural $n \in A$ o sucessor de n também está em A.

   Então A é o conjunto de todos os números naturais.

A forma em que Peano escreveu o sucessor de 1 foi como $1+1$, onde o símbolo $+$ não significa a *soma* de 1 mais 1, mas o *seguinte* de 1. É justamente a ideia intuitiva de acrescentar elementos de 1 em 1 a um conjunto inicial que tem um elemento, como ilustra a figura 1.1.

Porém, a forma de expressar historicamente a sequência de números naturais foi com o sistema decimal de numeração, o qual nos permite representar todos os números naturais mediante

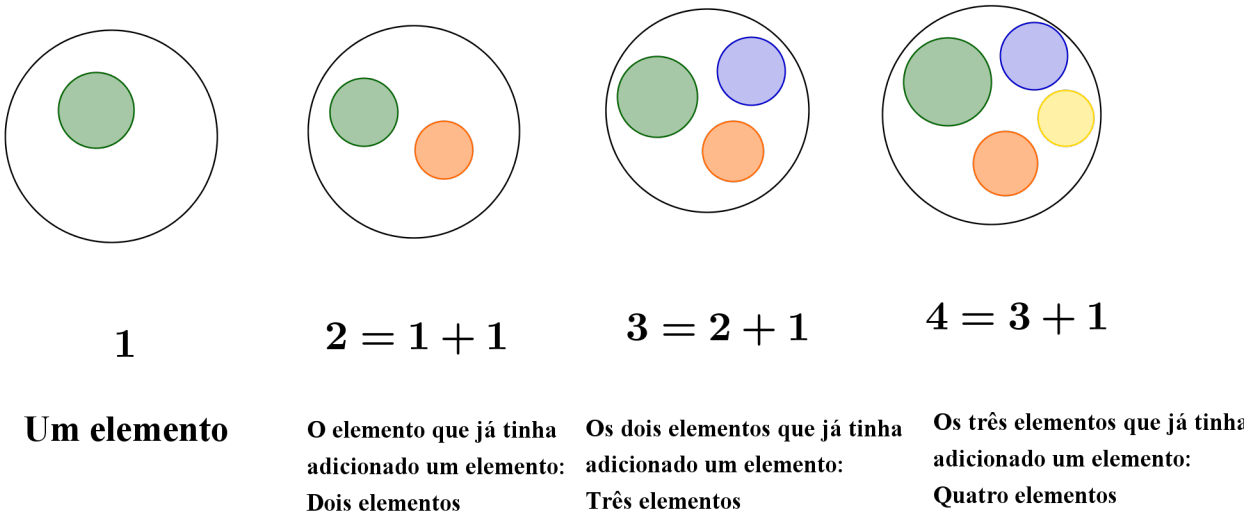


FIGURA 1.1: O número natural 1 e seus sucessores na contagem.

os

dígitos decimais $0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,$

Dessa forma, o homem consiguiu criar uma simbologia simples e fácil de memorizar de todos os sucessores do número 1, apenas com nove símbolos.

O quarto axioma de Peano se refere a uma carateristica única dos números naturais, que é a de ser um **conjunto indutivamente definido**. Esse axioma será explorado na seguinte subseção junto com o conhecido como princípio da Boa Ordenação. O essencial desse axioma é que está postulando a unicidade do conjunto que verifica os três primeiros axiomas e que este seja um conjunto indutivo. Portanto denotamos esse conjunto como $\mathbb{N}$.

Imaginamos que você esta familiarizado com o conceito de **função** e de **composição de funções**. A seguir, vamos definir funções com domínio em $\mathbb{N}$. Veremos que estas podem ser identificadas com "listas" infinitas de elementos. Antes, vamos definir o que é um conjunto indutivo de números naturais.

Definição 1.1. *Se A é um subconjunto de números naturais que verifica*

1. *existe $a > 1$ tal que $a \in A$;*
2. *para todo $n \geq a$ tal que $n \in A$, se verifica que $n + 1 \in A$,*

então o conjunto A é dito ser um conjunto indutivo iniciando em a.

Definição 1.2. *As funções que têm como domínio o conjunto dos números naturais ou um conjunto indutivo de números naturais a partir de* $a \neq 1$ *são chamadas de sequências .*

Exemplo 1.1. A função $f : \mathbb{N} \to \mathbb{N}$ tal que $f(n) = 2n$ é uma sequência, pois é uma função com domínio natural. Podemos ordenar as imagens em uma lista como segue:

$$\{2, 4, 6, \ldots, 2n, \ldots\},$$

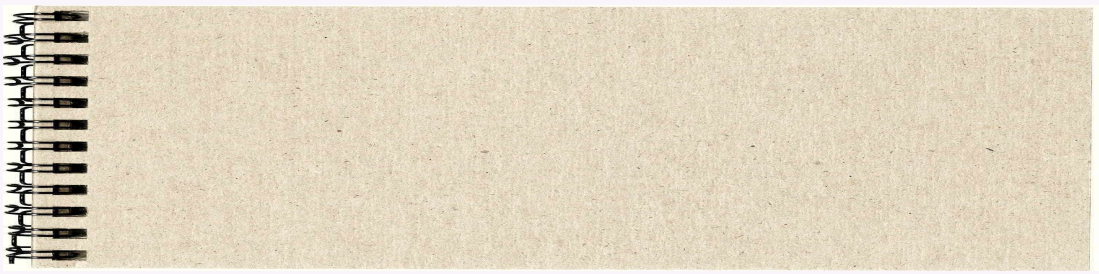
onde o primeiro elemento da lista é $f(1) = 2 \cdot 1$, o segundo elemento é $f(2) = 2 \cdot 2$ e assim sucessivamente.
Note que esta sequência está descrevendo o conjunto dos números pares.

Observação 1.1. Note que uma sequência não é outra coisa que uma lista ordenada de elementos extraídos de um conjunto imagem. A ordem na lista vem de acordo com o número que é a sua pré-imagem como $\{f(1), f(2), f(3), \ldots, f(n), \ldots\}$. Por isso é comum denotar à imagem de n como f_n.

Vamos apresentar o primeiro desafio para você. Lembre de não clicar na solução do desafio antes de ter pensado bem na solução. Assim o efeito do desafio será muito mais eficiente!

Desafio!

Escreva no caderno (note que é um caderno reciclável!) a sequência dos números ímpares de acordo com o feito no exercício 1.1.



Clique aqui para ver a resposta.

Definição 1.3. *Uma sequência é definida por recorrência se verifica quando*

1. *Conhece-se o valor de* $f(1)$*;*
2. *O valor de* $f(n+1)$ *é deduzido do o valor de* $f(n)$*.*

Exemplo 1.2. A função $f : \mathbb{N} \to \mathbb{N}$ definida da seguinte maneira:

$$g(0) = 1, \qquad g(n+1) = (n+1) \cdot g(n),$$

define o conhecido número $n!$. De fato, da definição temos que

$$\begin{aligned} g(1) &= (0+1) \cdot g(0) = 1 \cdot 1; \\ g(2) &= (1+1) \cdot g(1) = 2 \cdot 1; \\ g(3) &= (2+1) \cdot g(2) = 3 \cdot 2 \cdot 1; \\ g(4) &= (3+1) \cdot g(3) = 4 \cdot 3 \cdot 2 \cdot 1, \end{aligned}$$

Pesquise na internet sobre outros exemplos de funções definidas por recorrência. Faça um resumo do pesquisado leve-o no fórum de discussão.

Antes de continuar com a construção dos números naturais a partir dos axiomas de Peano, revisaremos (ou aprenderemos) alguns conceitos necessários para a melhor compreensão da teoria não só deste módulo mas também dos outros módulos do curso.

1.2 Alguns pré-requisitos

Algumas das ferramentas da teoria de conjuntos que vamos usar bastante no nosso curso serão revisadas nesta seção. A ideia é trazer à memória algumas definições ou apresentar outras que para o prezado aluno possam ser novidade.

1.2.1 Relações definidas em conjuntos

Nesta subseção iremos estudar a noção de relação binária entre conjuntos, operação binária, relação de ordem e de equivalência em um conjunto. Começaremos introduzindo o conceito de relação entre pares de conjuntos.

Definição 1.4. *Dados dois conjuntos, A e B, denotaremos por $A \times B$ o conjunto dos pares ordenados (a, b) tais que* ***a*** *pertence a A e b pertence ao conjunto B.*

Na figura 1.2 aparece uma representação gráfica do produto cartesiano.

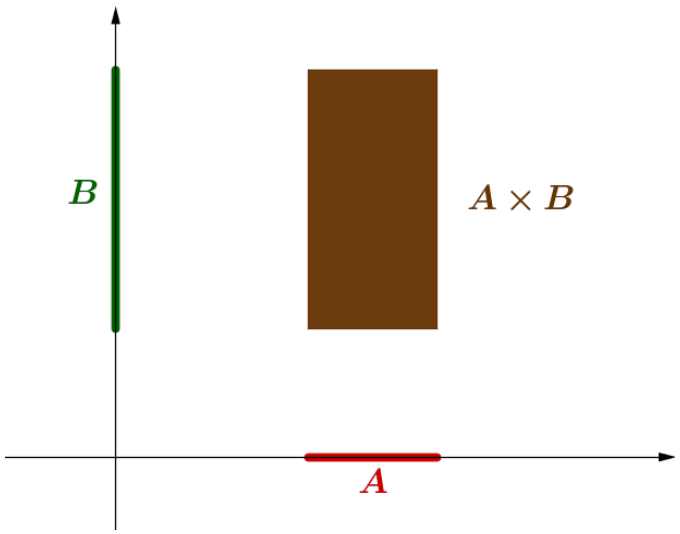


FIGURA 1.2: Uma visualização do produto cartesiano de conjuntos.

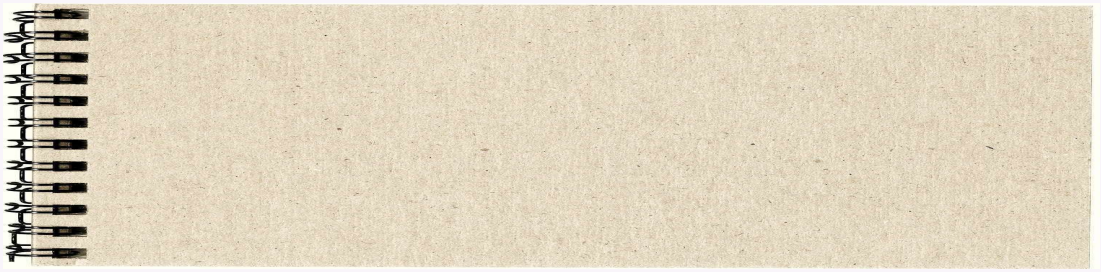
Definição 1.5. *Uma Relação Binária de um conjunto A em B é um subconjunto R de $A \times B$. Quando $(a, b) \in R$ diz-se que a está relacionado com b e denotamos por $a \; R \; b$.*

Exemplo 1.3. Seja o conjunto *A* dos países latinoamericanos e *C* o conjunto das capitais desses países latinoamericanos. Uma relação binária *R* entre *A* e *C* pode ser definida como

$$a \; R \; c \quad \textbf{se e somente se } c \text{ é capital de } a.$$

Desafio!

Escreva no caderno abaixo dois pares de elementos relacionados pela relação *R* definida no exemplo 1.3. Também escreva dois exemplos de pares que não pertencem à relação.



Clique aqui para ver uma resposta.

Podemos definir uma relação binária de um conjunto em si mesmo. Dado um conjunto *A* expressamos este tipo de relação binária de *A* em *A* como relação binária no conjunto *A*. Vamos ver alguns exemplos deste tipo de relações.

Exemplo 1.4. *No conjunto dos países do mundo e considerando que há cinco continentes, podemos relacionar os países por "pertencer ao mesmo continente". Assim, o par (Brasil,Uruguai) está nesta relação pois ambos os países pertencem ao continente americano. Também dizemos que Brasil está relacionado com Uruguai ou, sintéticamente, Brasil R Uruguai.*

Exemplo 1.5. *Uma relação matemática trivial em um conjunto A é dada por $R = \{(a, a), a \in A\}$. Portanto $a \ R \ b$ significa $a = b$.*

Definição 1.6. *Uma relação R em A se diz*

1. *Reflexiva: se para todo $a \in A$ temos $a \ R \ a$;*
2. *Simétrica: se cada vez que $a \ R \ b$ isto implica que $b \ R \ a$;*
3. *Antissimétrica: se ambas as afirmações $a \ R \ b$ e $b \ R \ a$ são verdadeiras, isto implica que a e b são o mesmo elemento;*
4. *Transitiva: se $a \ R \ b$ e $b \ R \ c$ temos também que $a \ R \ c$.*

Exemplo 1.6. A relação $\subset$ entre conjuntos não verifica a propriedade simétrica, mas verifica a propriedade antissimétrica.
De fato, o conjunto $A = \{1, 2\}$ é um subconjunto de $B = \{1, 2, 3\}$, mas isto não implica que B seja um subconjunto de A, o que mostra que $\subset$ não verifica a propriedade simétrica.
Por outro lado, se tivermos $M \subset N$ e $N \subset M$, temos que $M = N$, o que mostra que $\subset$ verifica a propriedade antissimétrica.

Definição 1.7. *Seja R uma relação binária definida no conjunto A. Então R é uma relação de ordem em A se verifica simultaneamente as propriedades reflexiva, antissimétrica e transitiva. O conjunto A com a relação de ordem R é dito de conjunto ordenado.*

Exemplo 1.7. A relação $\subset$ entre conjuntos é uma relação de ordem pois verifica as três propriedades. Com efeito, temos que $A \subset A$ para qualquer conjunto. Vimos no exemplo 1.6 que $\subset$ verifica a propriedade antissimétrica. Também, se $A \subset B$ e $B \subset C$ temos que $A \subset C$.

Definição 1.8. *Uma relação se diz de equivalência no conjunto A se for reflexiva, simétrica e transitiva. Quando R é uma relação de equivalência e tivermos $a\ R\ b$, diremos que a é equivalente a b e usaremos a notação $a \sim b$.*

Definição 1.9. *Seja R uma relação de equivalência definida em um conjunto A. Chamamos de classe de equivalência de $a \in A$ ao conjunto de todos os elementos $x \in A$ que são equivalentes a. Denotamos a classe de a como $[a]$*

Exemplo 1.8. No exemplo 1.4, a classe de equivalência [Brasil] é o conjunto

$$[\text{Brasil}] = \{P : \ P \quad \text{é um país do continente americano } \}.$$

Vamos demonstrar uma proposição que nos ajudará a agrupar os elementos de conjuntos "grandes" em um novo conjunto que é mais fácil de trabalhar. Isto será uma ferramenta poderosa no que segue deste módulo e no módulo III.

Proposição 1.1. *Seja o conjunto A e $\sim$ uma relação de equivalência definida em A. Dadas duas classes de equivalência $[a]$ e $[b]$ então se verifica que*

1. $[a] = [b]$ *ou* $[a] \cap [b] = \emptyset$;
2. *Para todo $a \in A$ existe uma classe à qual a pertence.*

Demonstração: Seja $c \in [a]$ e $c \in [b]$. Então temos por definição 1.9 que $c \sim a$ e $c \sim b$, de onde obtemos que $a \sim b$. Assim, $[a] = [b]$. Por outro lado, se $[b] \neq [a]$, suponha que existe $c \in A$ tal que $c \in [a] \cap [b]$. Isto significa que $c \sim a$ e que $c \sim b$. De onde, pela transitividade obtemos $a \sim b$, ou seja, $[a] = [b]$, pelo demonstrado anteriormente. Isto é uma contradição e completa a demonstração para o item 1.

O item 2 é consequência imediata da propriedade reflexiva da equivalência, já que todo elemento está *pelo menos* relacionado com si mesmo. ■

Observação 1.2. Todo elemento $b \in [a]$ pode ser um representante de uma classe de equivalência. Ou seja, se vamos tomar b como representante de $[a]$ devemos ter $b \sim a$.

Definição 1.10. *Seja o conjunto A e $\sim$ uma relação de equivalência definida em A. O conjunto quociente determinado pela relação $\sim$ é o conjunto de todas as classes de equivalência que denotamos por $A/\sim$. Simbolicamente:*

$$A/\sim = \bigcup_{a \in A} [a] \tag{1.1}$$

Note que, de acordo com a definição 1.10, cada elemento de A juntamente com seus equivalentes é um elemento de $A/\sim$. Para identificar um elemento de $A/\sim$ que é uma classe de um elemento de A, tomamos un representante qualquer dessa classe. Essa escolha depende de muitos fatores que veremos nas aplicações.

Exemplo 1.9. No exemplo 1.4 o conjunto quociente que determina a relação de equivalência R="mesmo continente" no conjunto P dos países do mundo é

$$P/\sim = \{[\text{Brasil}], [\text{Espanha}], [\text{África do Sul}], [\text{Austrália}], [\text{Índia}]\}.$$

Note que foi escolhido apenas um representante de cada continente para dar o nome à classe!

Na próxima definição vamos usar o conceito de função.

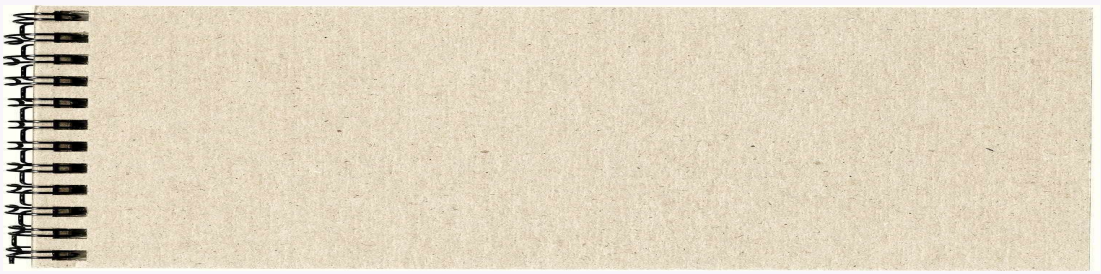
Definição 1.11. *Dado um conjunto A, uma operação binária $\star$ em A é uma função de $A \times A$ em A. Isto significa que, para cada par $(a, b) \in A \times A$, existe um único elemento $c \in A$ tal que $R((a, b)) = c$ e escrevemos $a \star b = c$.*

Observação 1.3. Note que da definição 1.11 surgem duas caraterísticas provenientes de operar a com b, que são: o *resultado* c é da mesma natureza que a e b, ou seja $c \in A$ e c é *único*.

Exemplo 1.10. A relação binária definida em $\mathbb{N}$ por $R((a, b)) = a - b$ não é uma operação binária, pois o par $(3, 4)$ não possui imagem no conjunto $\mathbb{N}$. Por isso dizemos que "$-$" não é uma operação (binária) em $\mathbb{N}$.

Desafio!

Seja o conjunto $X = \{\{1,\ 2\},\ \{1\},\ \{2\}\}$. Mostre que a união de conjuntos é uma operação binária em X.



Clique aqui para ver a resposta.

1.3 Operações binárias em $\mathbb{N}$

A adição e a multiplicação de números naturais são exemplos de funções definidas por recorrência. Vamos mostrar como definir a adição como ilustrativo da definição destas operações.

Lembrando que denotamos por $n+1$ o sucessor de n, a forma de adicionar será a mais intutitiva. Chamemos de s a função de $\mathbb{N}$ em $\mathbb{N}$ definida por

$$\begin{cases} s(1) = 1+1; \\ s(n+1) = s(n)+1. \end{cases}$$

Esta função é chamada de *função sucessor*, ou seja, está calculando o sucessor de cada número natural por recorrência (veja 1.3). Temos como consequência que $s(1) = 2$, $s(2) = 2+1 = 3$, $s(3) = 3+1 = 4$, $s(4) = 4+1 = 5$, e assim sucessivamente. Note que, por exemplo, as igualdades $s(1) = 2$ ou $s(2) = 2+1 = 3$ significam apenas que estamos usando o símbolo 2 para representar o sucessor de 1 e o símbolo 3 para o sucessor de 2 e assim sucessivamente.

Usando esta função podemos definir a operação de *adição* no conjunto dos números naturais. Para todo n e k números naturais define-se

$$\begin{cases} n+1 = s(n); \\ n+s(k) = s(n+k). \end{cases}$$

Portanto, $n+1$ é, por definição, o sucessor do número natural n. Por outro lado, conhecido o número natural $n+k$, saberemos o valor de $n+s(k)$ que será, também por definição, o número natural sucesspr de $n+k$. Usando as notações $n+1$ para o $s(n)$ e $(n+k)+1$ para $s(k+n)$, entederemos melhor o que a igualdade $(S2)$ significa que é

$$n+(k+1) = (k+n)+1,$$

muito mais familiar para nosso entendimento.

A definição de multiplicação por recorrência é feita também de uma maneira intuitiva: o produto de k por 1 é k e o produto de $n+1$ por k é $n \cdot k$ somado com k, recuperando assim o produto de k por qualquer número natural:

$$n \cdot k = \underbrace{k+k+\cdots+k}_{n \text{ somandos}},$$

muito bem conhecida.

Para provar as propriedades “clássicas” da adição e multiplicação - como comutativa, associativa, entre outras - se usa o que se conhece por Princípio de Indução, que está baseado no quarto axioma de Peano. Vamos ver esta forma de demonstração poderosa, que usaremos ao longo do curso na próxima subseção.

1.3.1 O Princípio de Indução no conjunto dos números naturais

Para entender o enunciado do princípio de indução, vamos primeiramente fazer algumas notações. Começemos com uma historinha inspiradora de uns dos gênios da humanidade.

O professor da escola de que participava o grande matemático alemão Karl Friedrich Gauss (1777 - 1855) quando tinha apenas sete anos de idade, pediu aos alunos que calculassem a soma dos inteiros de 1 a 100 como um desafio que imaginava ninguém iria responder... E poucos minutos depois de proposta, a genialidade de Gauss notou que a soma de $1 + 100$ é igual a de $2 + 99$ e assim por diante. Portanto, bastava somar os 50 números iguais a $1 + 100 = 101$, ou seja, a soma é $50 \cdot 101 = 5050$.

A formula de Gauss se generalizada na proposição 1.2.

Proposição 1.2. *A soma dos n primeiros números naturais é* $\dfrac{n(n+1)}{2}$.

Analisando a afirmação da proposição 1.2 com outros motivos, está se dizendo que se, por exemplo, tomarmos $n = 5$, a soma de $1 + 2 + 3 + 4 + 5$ é igual a calcular $\frac{5(5+1)}{2} = \frac{30}{2} = 15$. É verdade?

De fato, somando os 5 primeiros naturais obtemos o número 15. Dizemos então que a proposição é verdadeira para $n = 5$.

Será que a proposição 1.2 é verdadeira para $n = 10$?. Para isso teríamos que somar

$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10$$

e verificar que dá exatamente $\frac{10(10+1)}{2} = \frac{110}{2} = 55$ e que, de fato, é verdadeira.

Para facilitar as notações matemáticas desta subseção, lembremos que o símbolo $\sum$ representa matematicamente uma soma e é chamado de símbolo somatório. Por exemplo, quando escrevemos $\sum_{n=2}^{n=4} n^2 - 1$ representa a soma dos termos $(2^2 - 1) + (3^2 - 1) + (4^2 - 1)$.

Desafio!

Revise essas ideias desenvolvendo no caderno abaixo os somatórios e escrevendo simbolicamente em somatórios as somas indicadas.

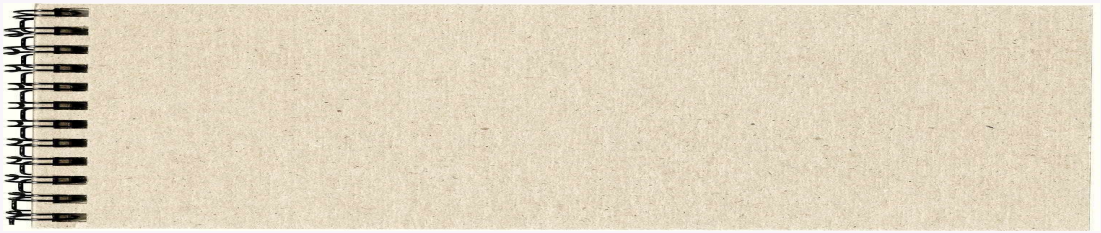
$$\sum_{i=2}^{i=4} \frac{i+1}{i-1} =; \quad 15 + 18 + 21 + 24 + 27 =.$$

$$\sum_{n=0}^{n=1} (n+1)n =; \quad \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} =$$

Também vamos adotar uma notação para expressar a proposição 1.2 e outras proposições relativas a números naturais de uma forma sintética. Por exemplo, para denotar a proposição 1.2 para o valor 5 em forma sintética, escrevemos $\mathcal{P}(5)$, significando com isso toda a expressão $1+2+3+4+5=\frac{5(5+1)}{2}$.

Desafio!

Escreva no caderno a proposição 1.2 para o valor 135 em forma estendida e em forma sintética usando o símbolo de somatório.



Clique aqui para ver a resposta.

Em geral, a proposição 1.2 escrita para n natural qualquer em forma sintética vem dada pela expressão $\mathcal{P}(n)$.

A seguir o enunciado do Princípio de Indução que escrevemos com a sigla PI.

O Princípio de Indução: Seja $\mathcal{P}(n)$ uma proposicão que depende do número natural n. Seja n_0 um número natural fixado. Tendo comprovado que

1. $\mathcal{P}(n_0)$ verdadeira.
2. Se $\mathcal{P}(n)$ é verdadeira para $n \geq n_0$ implica que $\mathcal{P}(n+1)$ é verdadeira.

Então $\mathcal{P}(n)$ é verdadeira para todo $n \geq n_0$.

Iremos utilizar muito o PI ao longo do nosso curso porque ele é uma ferramenta poderosa de demonstração de teoremas. O axioma quarto de Peano é chamado de Primeira forma do PI. O que está enunciado em 1.3.1 é o conhecido como princípio de indução completa.

Para começar a praticar o método, iremos demonstrar a proposição 1.2 usando o PI.

Exemplo do uso do Princípio de Indução (PI). Observe os passos lógicos que estão sendo usados.

Verificamos que $\mathcal{P}(1)$ é verdadeira, pois a soma se transforma apenas em um número que é o primeiro somando 1 e temos também que $\frac{1\cdot(1\cdot 2)}{2}=1$.

Agora tomamos um número n qualquer (não um caso particular) para o qual $\mathcal{P}(n)$ é verdadeira. Observe que esta afirmação, mesmo que de carater "geral", tem fundamento desde que

verificamos para um natural, no nosso caso o número 1. Temos então que para esse n vale que

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}, \tag{1.2}$$

e queremos demonstrar que

$$1 + 2 + \ldots + (n+1) = \frac{(n+1)(n+2)}{2}. \tag{1.3}$$

Partimos do membro à esquerda da igualdade (1.3):

$$\begin{aligned} 1 + 2 + \ldots + (n+1) &= 1 + 2 + \ldots + n + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1), \end{aligned}$$

onde aqui usamos (1.2). Agora, tirando denominador comum na última expressão, obtemos que

$$\begin{aligned} \frac{n(n+1)}{2} + (n+1) &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{n^2 + 3n + 2}{2} \\ &= \frac{(n+2)(n+1)}{2}, \end{aligned}$$

onde na última igualdade usamos a decomposição do polinômio $n^2 + 3n + 2$ em fatores $(n+2)$ $(n+1)$ a partir de suas duas raízes -2 e -1. Portanto demonstramos (1.3).

Faremos outro exemplo com uma proposição que envolve desigualdade. Veremos com mais detalhes o procedimento. Observe com atenção os passos para a demonstração por indução.

Proposição 1.3. *Seja n um número natural tal que $n \geq 5$ então $2^n > 5n$.*

Observação 1.4. Observe que a proposição está associada a números naturais *quaisquer*, apesar de que o enunciado pode sugerir que seja para um particular n.
Podemos, então, enunciar uma proposição $\mathcal{P}(n)$ referida aos números naturais que enuncia que $2^n > 5n$.

Demonstração: Consideremos a proposição $\mathcal{P}(n)$ que afirma que $2^n > 5n$. O primeiro número para o qual vamos checar se a proposição é verdadeira é $n_0 = 5$. Analisamos $\mathcal{P}(5)$ substituindo n_0 por 5 obtendo a proposição

$$\mathcal{P}(5) = 2^5 > 5 \cdot 5 \quad \text{é verdadeira.} \tag{1.4}$$

Como $2^5 = 32$ e $5 \cdot 5 = 25$, ou seja, a proposição afirma que $32 > 25$, concluindo que $\mathcal{P}(5)$ é verdadeira. Observe que para $n_0 = 4$ então $\mathcal{P}(4)$ é falsa porque temos $14.5 = 2^4 \not> 5 \cdot 4$.

Agora passaremos a demonstrar uma proposição que é conhecida como o teorema indutivo ou de indução, para completar a demonstração pelo método de indução.

Suponha que $\mathcal{P}(n)$ é verdadeira para n com a condição que $n \geq 5$. Esta seria nossa hipótese indutiva ou de indução. Em forma estendida,

$$\mathcal{P}(n) = 2^n > 5 \cdot n \quad \text{é verdadeira.} \tag{1.5}$$

Vamos mostrar com base na desigualdade (1.5) que $\mathcal{P}(n+1)$ é verdadeira, ou seja,

$$2^{n+1} > 5(n+1) \quad \text{é verdadeira.} \tag{1.6}$$

A proposição (1.6) é o que se conhece como tese indutiva ou de indução. Demonstrando agora (1.6), usamos (1.5) multiplicando ambos os membros por 2, obtendo

$$2^{n+1} > 10n. \tag{1.7}$$

Pela desigualdade (1.5)), temos que $n \geq 5$ e como consequência obtemos que $5n > 5$. Como temos que $10n = 5n + 5n$ e $n \geq 5$, podemos escrever

$$10n = 5n + 5n > 5n + 5 = 5(n+1).$$

Usando esta conclusão junto com (1.7), chegamos a que

$$2^{n+1} > 10n > 5(n+1),$$

ou seja, obtemos que $\mathcal{P}(n+1)$ é verdadeira.

Agora podemos usar o PI da seguinte maneira. A proposição $\mathcal{P}(5)$ é verdadeira. Pelo teorema de indução, temos que $\mathcal{P}(6)$ é verdadeira. Repetindo o procedimento para $7,\ 8,\ 9\ldots$, temos que a proposição $\mathcal{P}(n)$ será verdadeira para todo $n \geq 5$. ■

Analise a imagem da figura 1.3. É o chamado *efeito dominó* da demonstração por indução: se uma peça cai (proposição inicial verdadeira) e as outras são tais que seguem a regra (teorema indutivo) que se uma cai a seguinte também, então todas vão cair a partir da primeira!

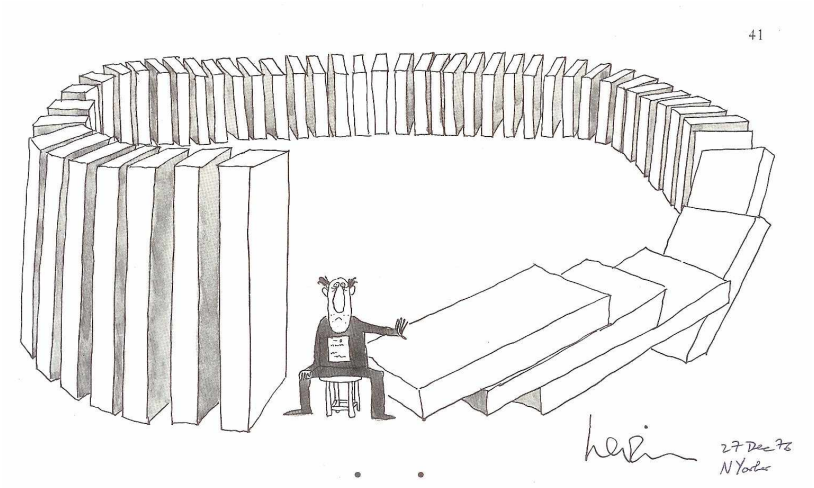


FIGURA 1.3: O Princípio de Indução. Imagem extraída do site http://www.cse.buffalo.edu/~rapaport/191/recursion.html

Observação 1.5. *Resumindo: o roteiro para demonstrar uma proposição pelo método de indução (ou usando o PI) é o seguinte:*

1. *Avalie a proposição (como verdadeira ou falsa) até que para um número natural seja verdadeira. Esse número será o que consideraremos como primeiro "a cair".*
2. *Formule o teorema de indução, supondo a proposição verdadeira para um natural a maior ou igual que o primeiro verificado (hipótese indutiva) e partindo dela verificar a tese indutiva, mostrando que a proposição é verdadeira para $n+1$. Este teorema não se demonstra para casos particulares mas sim em forma "geral".*
3. *Usamos sempre a hipótese de indução para, por meio de artificios, chegar a concluir a tese. Esta pequena demonstração é em geral a parte mais dificil do método. Com a prática se adquire a destreza!*

1.3.2 AS PROPRIEDADES DA ADIÇÃO E MULTIPLICAÇÃO EM $\mathbb{N}$

Imaginamos que você está habituado e conhece as propriedades básicas das operações de números naturais como, por exemplo, a propriedade que afirma que dado qualquer par de números naturais m e m tem-se

$$m+n=n+m \quad \text{e} \quad m\cdot n=n\cdot m.$$

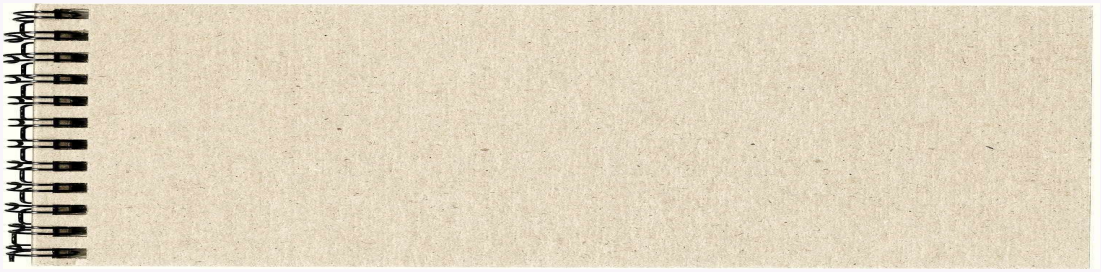
Essa propriedade é chamada de *propriedade comutativa* da operação.

Reflita: Imagine por um instante que você conhece tudo sobre números...a propriedade comutativa é verdadeira na operação de divisão de dois números?

Compreende a pergunta? Especificando melhor com um exemplo, note que o resultado de dividir 10 entre 5 não é a mesma coisa que o resultado de dividir 5 entre 10. Logo, a divisão não tem a propriedade comutativa.

Desafio!

Escreva também outro exemplo de uma operação de números conhecida por você que **não** tem a propriedade comutativa.



Clique aqui para ver uma resposta.

As propiedades da adição e multiplicação em $\mathbb{N}$ são enunciadas a seguir.

Propriedades 1.1. *Para todo m, n e p números naturais tem-se*

1. *Associativa:* $m + (n + p) = (m + n) + p$ *e* $m \cdot (n \cdot p) = (m \cdot n) \cdot p$;
2. *Comutativa:* $m + n = n + m$ *e* $m \cdot n = n \cdot m$;
3. *Lei do Cancelamento:* $m + n = m + p$ *implica* $n = p$ *e* $m \cdot n = m \cdot p$ *implica* $n = p$;
4. *Distributiva da multiplicação com respeito à adição:* $m \cdot (n + p) = m \cdot n + m \cdot p$.

Vamos demonstrar a propriedade comutativa da adição para ilustrar mais uma vez o método

de indução. Estamos supondo também que a propriedade associativa é verdadeira.

Demonstração: (Demonstração da propriedade comutativa da adição)

Vamos checar que a propriedade é válida para $n = 1$, lembrando que, por definição de adição, temos que

$$(n + k) + 1 = n + (k + 1),$$

que é a mesma coisa que dizer que o sucessor de $n + k$ é n somado com o sucessor de k. Logo, temos que para $n = 1$ é verdadeiro que

$$(n + 1) + 1 = n + (1 + 1).$$

Isto prova a primeira parte da demonstração por indução.

Suponha que $n + k = k + n$. Vamos provar que $n + (k + 1) = (k + 1) + n$. Então,

$$\begin{array}{rcll} n + (k + 1) & = & (n + k) + 1 & \text{pela definição de adição} \\ & = & (k + n) + 1 & \text{pela hipótese inductiva} \\ & = & k + (n + 1) & \text{pela propriedade associativa} \\ & = & k + (1 + n) & \text{pela primeira parte da indução} \\ & = & (k + 1) + n & \text{pela propriedade associativa,} \end{array}$$

o que mostra a propriedade. ■

Da mesma forma se demonstram as propriedades da adição e multiplicação. Vamos supor que já fizemos a tarefa e continuamos nosso caminho para usar mais uma vez o PI, que é relacionado com a *Potenciação de expoente natural*.

Definição 1.12. *Potência de expoente natural. Dados $a \in \mathbb{N}$ e $n \in \mathbb{N}$ definimos potência de base a e expoente n por recorrência (veja 1.3)*

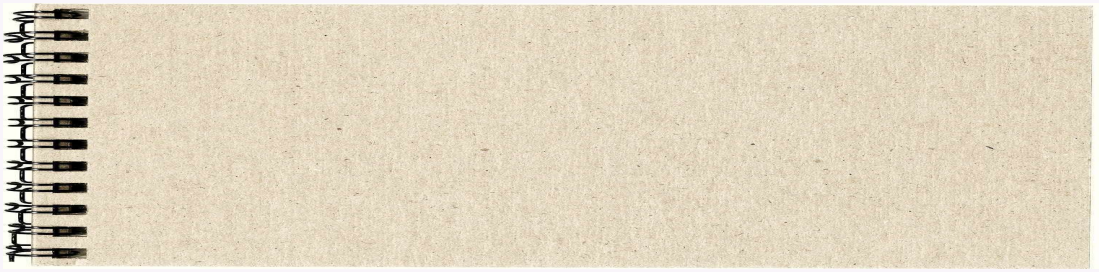
$$a^1 = a \quad \text{e} \quad a^{n+1} = a \cdot a^n. \tag{1.8}$$

Vemos que usando a recorrência chegamos à "classica" definição de potenciação:

$$a^n = \underbrace{a \cdot a \cdots a}_{n \text{ fatores}}. \tag{1.9}$$

Desafio!

Mostre a partir de (1.8) que (1.9) é verdadeira.



Clique aqui para ver a resposta.

Proposição 1.4 (Propriedades da Potenciação). *As seguintes afirmações são verdadeiras para todo* $a,\ b,\ c$ *inteiros e* $m,\ n$ *naturais.*

1. $(ab)^n = a^n \cdot b^n$;
2. $(a^n)^m = a^{nm}$;
3. $a^n \cdot a^m = a^{n+m}$;
4. *sendo* $a < b$ *implica* $a^n < b^n$;
5. *sendo* $n > m$ *temos que* $a^n \geq a^m$;

Vamos demonstrar o item 3 da proposição 1.4 usando o princípio de indução.

Proposição 1.5. *Seja* m *um número natural. Então* $\mathcal{P}(n):\ \ a^n \cdot a^m = a^{n+m}$ *é verdadeira para todo* $n \in \mathbb{N}$.

Demonstração: Verificamos $\mathcal{P}(n)$ para $n = 1$. Temos que

$$a^1 \cdot a^m = a \cdot a^m = a^{m+1},$$

comprovando que $\mathcal{P}(1)$ é verdadeira.

A seguir demonstramos o teorema indutivo:

Hipotese: $\mathcal{P}(n)$ é verdadeira

Tese: $\mathcal{P}(n+1)$ é verdadeira, que é equivalente a mostrar $a^{n+1} \cdot a^m = a^{(n+1)+m}$.

Para demonstrar a tese, partimos da hipótese que afirma que $a^n \cdot a^m = a^{n+m}$ é verdadeira.

Demonstrando o teorema indutivo:

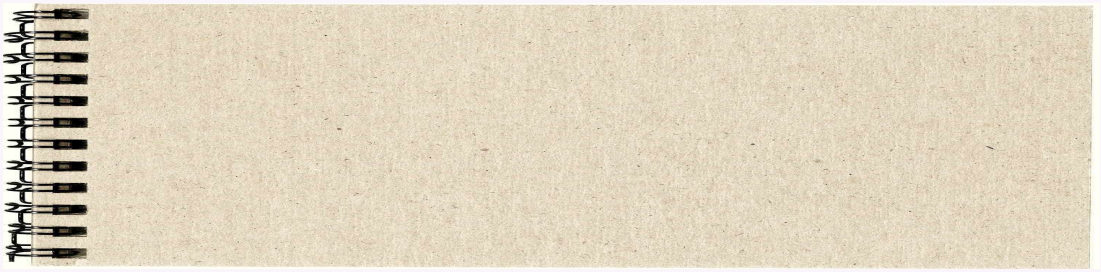
$$\begin{aligned} a^{n+1} \cdot a^m &= (a \cdot a^n) \cdot a^m && \text{usando a definição de potenciação} \\ &= a \cdot a^{n+m} && \text{usando associativa do produto e a hipótese indutiva} \\ &= a^{(n+m)+1} && \text{aplicando a definição de potenciação} \\ &= a^{(n+1)+m} && \text{usando a comutativa e associativa da adição,} \end{aligned}$$

de onde obtemos a tese indutiva.

Desta maneira a propriedade é verdadeira para todo $n \in \mathbb{N}$. ■

Desafio!

Mostre a propriedade do item 1 de potenciação.



Clique aqui para ver a resposta.

1.3.3 Relação de ordem em $\mathbb{N}$

A adição de números naturais permite introduzir uma relação de ordem em $\mathbb{N}$ que definimos a seguir.

Definição 1.13. *Sejam m e n números naturais. Denotamos $m > n$ e dizemos que m é maior que n, se existir k natural tal que $m = n + k$.*
Denotamos $n < m$ quando $m > n$. Também denotamos que $m \geq n$ se $m > n$ ou $m = n$.

Observação 1.6. Note que da definição 1.13 temos que $m + 1 > m$ (aqui o k da definição é 1). Isto implica, pelo axioma 3 de Peano, que 1 é o menor dos números naturais.

A relação R entre dois naturais definida por $n \; R \; m$ se e somente se $n > m$ ou $n = m$ é uma relação de ordem em $\mathbb{N}$ (veja definição 1.7). Não é difícil ver que as propriedades reflexiva e antissimétrica são verdadeiras. Vamos ilustrar como provar a propriedade transitiva da relação de ordem.

Proposição 1.6. *Dados $m,\ n$, e p em $\mathbb{N}$ onde $p \geq n$ e $n \geq m$. Então $p \geq m$.*

Demonstração: Temos por hipótese que existem k e r números naturais tais que $n = m + k$ e $p = n + r$. Assim, temos que $p = (m + k) + r = m + (k + r)$ e portanto existe o número

natural $l = k + r$ tal que $p = m + l$, o que significa, pela definição 1.13, que $p > m$. ■

Desafio!

Demonstre a propriedade antissimétrica da relação de ordem em $\mathbb{N}$.

Clique aqui para ver a resposta.

Outras duas importantes propriedades que se deduzem da definição de ordem no conjunto dos números naturais são as propriedades relativas a uma ordem e de compatibilidade com as operações estabelecidas em $\mathbb{N}$. Enunciaremos estas propriedades sem fazer a sua demonstração.

Propriedades 1.2 (Propriedades da relação de ordem em $\mathbb{N}$)**.** *Para m, n, e p em $\mathbb{N}$ verifica-se*

1. *Tricotomia: se $m \neq n$ então $m > n$ ou se isto é falso, temos que $n > m$.*
2. *Monotonia: se $m > n$ então $m + p > n + p$ e $mp > np$.*

Uma consequência das propriedades da relação de ordem é a propriedade 1.7, que afirma que, entre dois números naturais consecutivos, n e $n + 1$, não há números naturais.

Proposição 1.7. *Dado $n \in \mathbb{N}$ então* **não existe** *$p \in \mathbb{N}$ tal que $n < p$ e ao mesmo tempo $p < n + 1$.*

Demonstração: Suponha que existisse p tal que $n < p$ e $p < n + 1$. Então para algum k e r naturais teríamos $p = n + k$ e $n + 1 = p + r$. Portanto, $n + 1 = n + k + r$ e como consequência $1 = k + r$, que significa que $k < 1$. Isto é uma contradição, já que k é um número natural diferente de 1 e portanto tem que ser maior que 1. ■

Vamos "visualizar" esta ideia de ordem no conjunto dos números naturais, colocando-os em uma reta marcando o ponto de partida em 1 e organizando os sucessores à direita e antecedentes à esquerda, como mostra a figura 1.4.

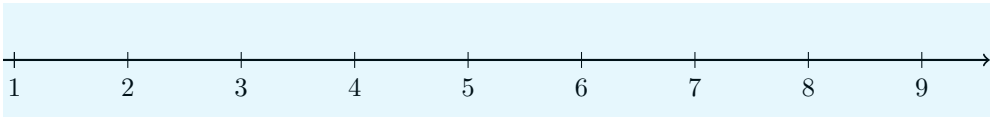


FIGURA 1.4: A visualização da ordem dos números naturais na reta.

1.3.4 PRINCÍPIO DA BOA ORDENAÇÃO

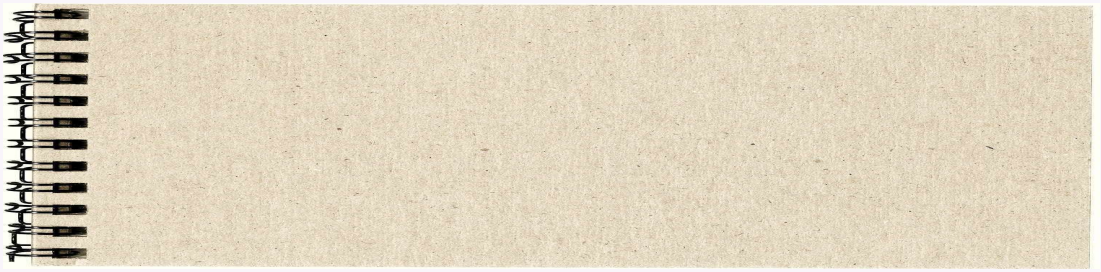
A seguir vamos definir alguns conceitos que usaremos no enunciado do princípio da boa ordenação.

Definição 1.14. *Diz-se que* $m \in \mathbb{N}$ *é o* mínimo *de um conjunto* $A \subset \mathbb{N}$ *se* $m \leq a$ *para todo* $a \in A$.

Exemplo 1.11. Vamos considerar o conjunto $A = \{3, 10, 4, 100, 12\}$. Temos que $3 < 10$, $3 < 4$, $3 < 100$ e $3 < 12$ além que $3 \leq 3$. Assim checamos que 3 é menor que TODOS os elementos de A, então pela definição 1.14, 3 é o mínimo de A.

Desafio!

Escreva no caderno abaixo a definição de *máximo* de um conjunto $A \subset \mathbb{N}$ e apresente um exemplo similar ao 1.11. Não esqueça de checar a propriedade de ser "maior" com TODOS os elementos do conjunto!



Clique aqui para ver a resposta.

As propriedades da relação de ordem em $\mathbb{N}$ são válidas para outros conjuntos numéricos como os números inteiros e racionais. A propriedade que enunciaremos no teorema 1.1 a seguir só é válida para a ordem entre os números naturais, logo não se encontra outra igual para os números inteiros, racionais ou reais.

Teorema 1.1 (Princípio da Boa Ordenação)**.** *Todo subconjunto não-vazio de* $\mathbb{N}$ *possui um elemento mínimo.*

Demonstração: No caso que $1 \in A$ então o teorema está provado. Suponha agora que $1 \notin A$. Vamos considerar o conjunto $X \subset \mathbb{N}$ dos naturais com a seguinte propriedade:

$$\mathcal{P}(n) : n \geq k \text{ para todo } k \notin A.$$

Em outras palavras, n verifica que todos os números menores que este número não pertencem a A. Se fosse $X = \mathbb{N}$, concluiríamos que $A = \emptyset$, o que é uma contradição. Logo, pelo axioma 4 de Peano (veja 1.1, pag. 18), deve existir algum natural n_0 tal que $n_0 \in X$ mas $n_0 + 1 \notin X$. Isso significa que $n_0 + 1 \in A$ e para todo $k < n_0 + 1$, $k \notin A$. Portanto todo elemento de A tem que ser maior ou igual que $n_0 + 1$, mostrando que este número é o mínimo do conjunto A. ■

Uma aplicação do Princípio da Boa Ordenação, que será usada no módulo 4, é a enunciada na proposição 1.8 a seguir.

Proposição 1.8. *Toda função monótona não crescente* $f : \mathbb{N} \to \mathbb{N}$ *é constante a partir de um certo valor natural, ou seja, existe* k *natural tal que* $f(n) = f(k)$ *para todo* $n \geq k$*.*

Demonstração: Temos que o conjunto $X = \{f(1), f(2), \ldots, f(n), \ldots\}$ é um conjunto de numeros naturais não vazio. Então pelo princípio da boa ordenação deve existir m o mínimo de X. Assim para todo $n > k$ devemos ter $f(n) \leq f(k) = m$, pois f é uma função não crescente. Assim concluímos que $f(n) = f(k)$ para todo $n > k$.

■

Corolario 1.1. *Toda sequência de números naturais decrescente, isto é, verifica-se* $n_1 > n_2 > \cdots$*, é constante a partir de um número* k *natural.*

1.4 Números Inteiros

Desde a escola notamos que um número inteiro negativo pode ser definido como a diferença de dois números naturais, como por exemplo $-1 = 2 - 3$.

Este fato nos dá uma motivação para fazer uma construção formal dos números inteiros a partir dos números naturais. Estamos, em uma palavra, estendendo o conjunto dos números naturais para obter uma operação binária entre os números naturais tais que $a < b$.

O que vamos fazer é associar ao número -1 o par ordenado de números naturais que lhe deu origem $(2, 3)$. O problema desta associação é que não existe um único par que dá origem ao número -1. Outros pares ordenados seriam $(4, 5)$, $(101, 102)$ e assim por diante. Então a questão é...

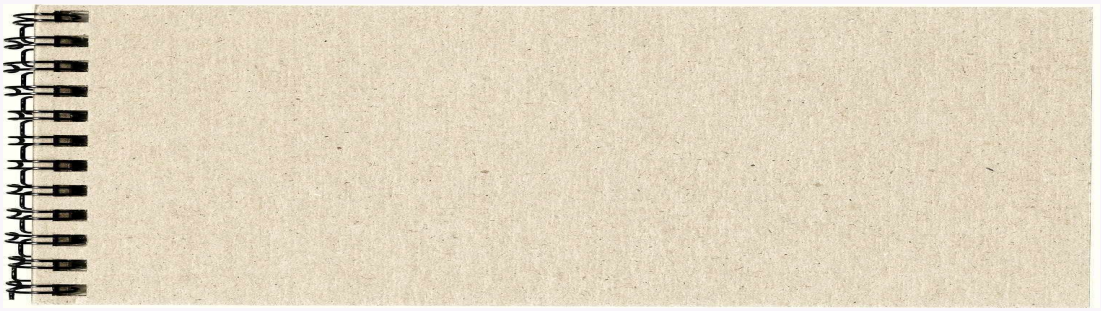
... de que forma podemos definir o número -1 sem lugar a dúvidas?

A resposta que os matemáticos encontraram para esta questão é estabelecendo uma relação entre os pares ordenados de números naturais de maneira que seja uma relação de equivalência (veja 1.8, pag. 24). Dados $m,\ n,\ m'$ e n' números naturais então

$$(m,n)R(m',n') \quad \text{se e somente se} \quad m = n \quad \text{ou} \quad m - n = m' - n'. \tag{1.10}$$

Desafio!

Mostre que a relação definida em 1.10 é de fato uma relação de equivalência.



Clique aqui para ver a resposta.

Assim a relação R, que denotaremos $\sim$ por ser uma relação de equivalência, determina uma partição de $\mathbb{N}$ em classes de equivalência, cada uma das quais define um único número inteiro. Denotamos por $\mathbb{Z}$ ao conjunto quociente (veja 1.10, pag. 25) de todas as classes de equivalências, isto é,

$$\mathbb{Z} = \{[(m,n)],\ m,\ n \in \mathbb{N}\}, \tag{1.11}$$

e qualquer número inteiro z é da forma $z = [(m,n)]$ com m e n números naturais.

Notação 1.1. O número inteiro determinado pela classe do par ordenado $(1,1)$ o denotaremos como 0.

Dado $z = [m,n]$ então se $m \neq n$ temos, pela tricotomia da relação de ordem nos números naturais (veja 1.2, pag. 37), duas possibilidades que analisamos como segue:

1. se $m > n$ existe um numero natural p tal que $m = n + p$. Identificamos z com p uma função bijetiva $f : \mathbb{N} \to \mathbb{Z}$ tal que $f(n) = [(n+p, n)]$ e denotamos $[(n+p, n)] = p$

2. se $n > m$ existe um numero natural r tal que $n = m + r$. Denotamos $(m, m+r)] = -r$.

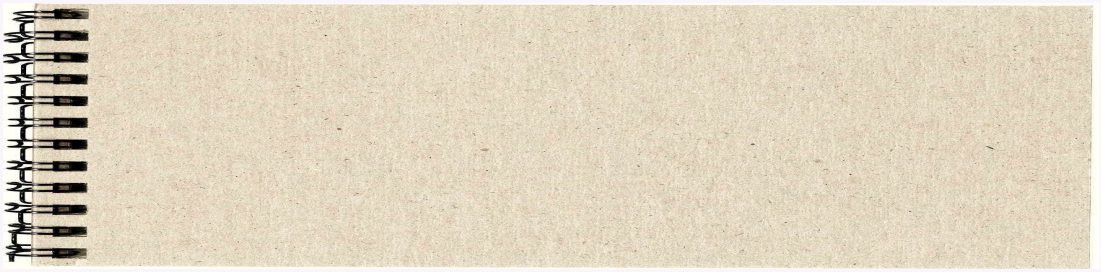
Observação 1.7. *Note que com a bijeção f definida acima temos que*

$$\mathbb{N} \subset \mathbb{Z}.$$

Exemplo 1.12. Identifiquemos os inteiros representados por pares ordenados de números naturais pela sua notação. A classe $[(9,5)]$ corresponde ao inteiro $[(4+5, 5)]$ e temos a identificação pela bijeção com com o número natural 4, portanto, $[(9,5)] = 4$. O inteiro $z = [(3,10)]$ é igual a $[(3, 3+7)]$ e sendo 10 a segunda componente com $10 > 3$, temos que $[(3,10)] = -7$.

Desafio!

Ache as notações para os inteiros $z_1 = [(130,2)]$, $z_2 = [(1,8)]$, $z_3 = [(1400,1400)]$ e $z_4 = [(60,61)]$.



Clique aqui para ver a resposta.

1.4.1 Operações no conjunto dos números inteiros

Vamos definir adição de inteiros a partir de suas classes de equivalência $[(m,n)]$ e $[(m_1,n_1)]$, com $m,\ m_1,\ n,\ n_1 \in \mathbb{N}$.

Definição 1.15.

$$[(m,n)] + [(m_1,n_1)] = [(m+m_1, n+n_1)]. \tag{1.12}$$

Observação 1.8. Note que, pela forma que estamos identificando os inteiros que já conhecemos de muito tempo com as classes de equivalência, temos que o inteiro definido pela equação (1.12) viria confirmar a igualdade $(m-n)+(m_1-n_1) = (m+m_1)-(n+n_1)$.

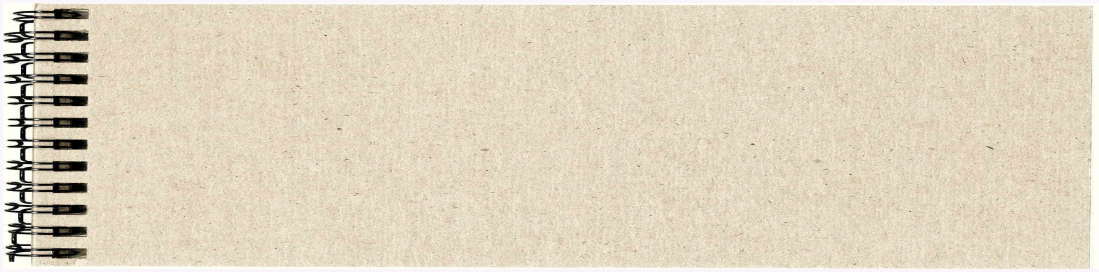
Exemplo 1.13. Para adicionar o inteiro $z_1 = [(2,5)]$ a $z_2 = [(2,1)]$, faríamos pela equação (1.12)

$$z_1 + z_2 = [(2,5)] + [(2,1)] = [(4,6)]$$

que, pela observação 1.6, seria na linguagem cotidiana o número inteiro $4-6$, que é -2.

Desafio!

Ache o resultado (soma) da adição dos pares $z_1 = [(122,55)]$ e $z_2 = [(202,11)]$, $z_3 = [(12,45)]$ e $z_4 = [(1,10)]$ de acordo com a definição 1.15 e anote-os de acordo com a observação 1.6.



Clique aqui para ver a resposta.

Vamos provar que esta operação está bem definida no sentido que o resultado não depende dos representates das clases de equivalências que se escolham para adicionar. Em outras palavras, demonstramos a seguinte proposição.

Proposição 1.9. *Dados os números inteiros* $z_1 = [(m_1, n_1)]$ *e* $z_2 = [(m_1', n_1')]$. *Suponha que* $(m_1, n_1) \sim (m_2, n_2)$ *e* $(m_1', n_1') \sim (m_2', n_2')$, *então temos que*

$$(m_1 + m_1', n_1 + n_1') \sim (m_2 + m_2', n_2 + n_2'). \tag{1.13}$$

Demonstração: Das equivalências da hipótese obtemos as igualdades

$$m_1 + n_2 = m_2 + n_1 \quad \text{e} \quad m_1' + n_2' = m_2' + n_1',$$

de onde obtemos

$$m_1 + m_1' + n_2 + n_2' = m_2 + m_2' + n_1 + n_1',$$

ou equivalentemente

$$m_1 + m_1' - (n_1 + n_1') = m_2 + m_2' - (n_2 + n_2'),$$

que pela definição 1.15 significa exatamente 1.13. ■

Observação 1.9.
Note que se efetuarmos a adição $[(4, 8)] + [(8, 4)]$ o resultado é $[(12, 12)] = 0$, isto pela notação que combinamos em 1.1.
De modo geral, temos que, para $m,\ n$ números naturais, é verdadeiro que

$$[(m, n)] + [(n, m)] = [(m + n, m + n)] = 0.$$

Além disso, note que em

$$[(m, n)] + [(n, n)] = [(m + n, n + n)] = [(m, n)], \tag{1.14}$$

a última igualdade é justificada pelo fato de que $(m + n, n + n) \sim (m, n)$ pois $m + n - (n + n) = m - n$.

Vamos continuar com uma definição que se refere a conceitos gerais como o de **estruturas algébricas**, **grupo** e **corpo**.

Definição 1.16. *Em um conjunto A onde se tenha estabelecido uma operação binária $\bigstar$ para a qual existe um elemento $n \in A$ tal que*

$$a \bigstar n = n \bigstar a = a \quad \text{para todo } a \in A, \tag{1.15}$$

então o elemento n é chamado de neutro da operação $\bigstar$.
Verificando-se que para cada elemento de $a \in A$ existe um elemento a' tal que

$$a \bigstar a' = a' \bigstar a = n \quad \text{para todo } a \in A, \text{ onde } n \text{ é neutro de } \bigstar \tag{1.16}$$

então o elemento a' é chamado de simétrico de a pela operação $\bigstar$.
Note que o simétrico do neutro é o próprio neutro pois $n \bigstar n = n$.

Temos observado na observação 1.9, que o número inteiro 0 é neutro da operação adição, sendo o único inteiro que verifica isso. Em 1.9 também foi notado que todo número inteiro tem simétrico com respeito à adição. Ao simétrico de um inteiro z pela operação adição é comum chamá-lo de oposto de z. Mais uma conclusão da observação 1.9 é que se $m = n + p$, $m,\ n$ e p números naturais, então $p = [(m, n)],\ -p = [(n, m)]$. Portanto

$$p + (-p) = 0, \tag{1.17}$$

que imaginamos não deve ser muito surprendente para o leitor!
Com um pouco de trabalho podemos demonstrar que a adição em $\mathbb{Z}$ verifica as propriedades associativa e comutativa além das mencionadas na definição 1.16.

Propriedades 1.3 (Propriedades da adição de números inteiros)**.** Para todo a, b e c números inteiros se verificam as seguintes propriedades:

1. Associativa: $(a + b) + c = a + (b + c)$;
2. Comutativa: $a + b = b + a$;
3. Existência de Neutro: O número 0 é o único inteiro que verifica que $a + 0 = a$ para todo $a \in \mathbb{Z}$.
4. Existência de Oposto: Para cada número inteiro a existe um número inteiro $a' = -a$ que verifica
$$a + a' = 0. \tag{1.18}$$

Como já fizemos anteriormente, *reflita* se a divisão de números possui as propriedades de neutro e oposto que enunciamos da adição de números inteiros.

A partir da existência de oposto para todo número inteiro, faz sentido fazer a seguinte definição da operação "inversa" da adição.

Definição 1.17. *Subtração: Dados a e b números inteiros definimos*

$$a - b = a + b', \text{ onde } b' \text{ é o oposto de } b.$$

Observação 1.10. *Note que*

$$z - z = z + (-z) = 0.$$

Ou seja, o fato de que um número inteiro menos ele mesmo é zero não é outra coisa que uma consequência da propriedade do oposto da operação adição!

1.4.2 Relação de ordem no conjunto dos números inteiros

A definição que vamos adotar para definir uma relação de ordem em $\mathbb{Z}$ vai ser a mesma que fizemos no conjunto dos números naturais. Ou seja, vamos "colar e copiar" a definição 1.13 exceto que consideraremos dois inteiros a e b para comparar.

Definição 1.18. *Sejam a e b números inteiros. Denotamos $a > b$ e dizemos que a é maior que b, se existir k, número natural, tal que $a = b + k$.*
Denotamos, como no conjunto dos números naturais, que $a < b$ quando $b > a$ e $b \geq a$ quando $b > a$ ou $b = a$.

Note que pela definição 1.18 obtemos que

$1 > 0$ porque existe o número natural 1 tal que $1 = 0 + 1$.

Também concluímos que se $a > 0$ então a pode ser identificado com um número natural, pois $a = 0 + a$.

Além disso, $0 > b$ se existir um número natural p tal que $0 = b + p$. Ora, pela unicidade do oposto do número b, devemos ter $-b = p$. Note também que, do fato que $0 > b$ e $0 = b + p$ para algum p natural, temos que $0 - b = p \in \mathbb{N}$. Assim, todo número inteiro da forma $0 - b$ com $0 > b$ é um número natural.

Estas considerações justificam porque geometricamente representamos a reta inteira como na figura 1.5.

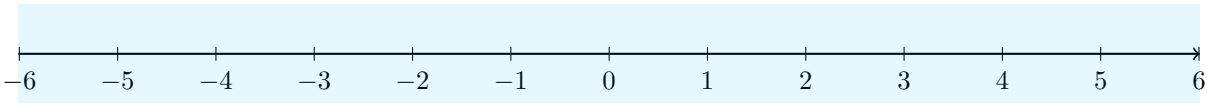


FIGURA 1.5: A visualização da ordem dos números inteiros na reta.

Da definição 1.18 pode-se demonstrar que de fato a relação $>$ é uma relação de ordem (veja 1.7) como também as seguintes propriedades.

Propriedades 1.4 (Propriedades da relação de ordem em $\mathbb{Z}$)**.** *Para a, b, e c em $\mathbb{Z}$ verifica-se*

1. *Transitiva: Se $a < b$ e $b < c$, então $a < c$.*
2. *Monotonia:*
   - *(a) se $a < b$ então $a + c < b + c$;*
   - *(b) se $a < b$ e $0 < c$ então $ac < bc$;*
   - *(c) se $a < b$ e $c < 0$ então $bc < ac$.*

Uma outra propriedade que é consequência da definição de adição e da relação de ordem é a conhecida regra dos sinais tanto para a adição como para a multiplicação que veremos mais adiante. Primeiramente algumas notações.

Notação 1.2. Denotamos por $\mathbb{Z}^+ = \{z \in \mathbb{Z},\ z > 0\}$, que denominamos como conjunto dos **números inteiros positivos** e que, por sua vez, estamos identificando com o conjunto dos números naturais.
Também denotamos por $\mathbb{Z}^- = \{z \in \mathbb{Z},\ z < 0\}$, que denominamos como conjunto dos **números inteiros negativos**.

Proposição 1.10. *Se a e b pertencem a $\mathbb{Z}^+$ então $a+b \in \mathbb{Z}^+$. Também, se a e b pertencem a $\mathbb{Z}^-$ então $a+b \in \mathbb{Z}^-$.*

Demonstração: Que a proposição é verdadeira para $\mathbb{Z}^+$ é claro. Vamos provar para $\mathbb{Z}^-$. De que $a,\ b \in \mathbb{Z}^-$ então existem naturais p e q tais que $0 = a+p$ e $0 = b+q$ de onde $0 = (a+b)+(p+q)$ com $p+q \in \mathbb{N}$. Então, pela definição 1.18 temos que $0 > a+b$, o que prova o afirmado. ■

Observação 1.11. Por causa das afirmações da proposição, diz-se que os conjuntos $\mathbb{Z}^+$ e $\mathbb{Z}^-$ são fechados com respeito à operação de adição.

Você lembra o que, geometricamente falando, os números inteiros 1 e -1 têm em comum?

A resposta é o fato de estarem à mesma *distância* de 0, lembrou?. A distância de um número qualquer ao zero é o que chamamos de valor absoluto do número. Você pode visualizar na figura 1.6 esta interpretação geométrica.

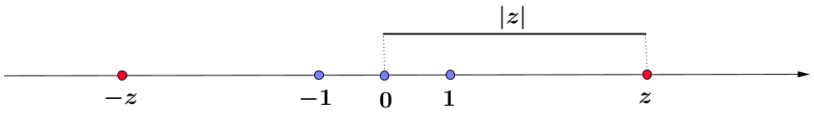


FIGURA 1.6: A interpretação geométrica na reta do valor absoluto.

A seguir vamos definir o que é o valor absoluto de um número inteiro. Note que é a mesma definição que você já viu nos cursos de cálculo!

Definição 1.19. *Dado $z \in \mathbb{Z}$ denotamos $|z|$ ao valor absoluto de z definido como*

$$|z| = \begin{cases} z, \text{ se } z \geq 0; \\ -z, \text{ se } z < 0. \end{cases} \tag{1.19}$$

Temos então que números inteiros que são opostos têm o mesmo valor absoluto. Em símbolos: $|z| = |-z|$.

1.4.3 A MULTIPLICAÇÃO NO CONJUNTO DOS NÚMEROS INTEIROS

Qual é a diferença entre multiplicar números naturais e inteiros? Lembre que para multiplicar dois números naturais $m \cdot n$ era preciso transformá-los em uma adição de m parcelas iguais a n. Por exemplo, multiplicar $4 \cdot 2$ é efetuar a soma $4 + 4$ ou $2 + 2 + 2 + 2$.

Como interpretaremos então o que significa multiplicar $a \cdot b$ sendo a e b números inteiros?

Lembre que a capacidade de contagem vem da parte dos números naturais. Portanto teríamos resolvido o problema teórico de como definir o produto de, por exemplo, $(-4) \cdot 2$, pois seria somar duas vezes o inteiro -4. Note também que, como soma de números inteiros negativos dá como resultado um número inteiro negativo (veja 1.10, pag. 47) então o resultado desta multiplicação é um número inteiro negativo.

E como resolveríamos o problema teórico para ambos os números inteiros negativos?

Vejamos novamente isto com um exemplo. Queremos multiplicar $(-4) \cdot (-2)$. Sabemos da escola que o resultado é 8, que é o resultado de $4 \cdot 2$. Portanto $(-4) \cdot (-2)$ é o mesmo que o produto dos seus opostos naturais.

Resumimos estas conclusões na seguinte definição.

Definição 1.20. *Dados números inteiros a e b definimos a operação multiplicação como*

1. *se $a, b \in \mathbb{Z}^+$ é uma multiplicação de números naturais tal que $a \cdot b = \underbrace{a + \ldots + a}_{b \text{ parcelas}}$.*
2. *se $a \in \mathbb{Z}^-$ e $b \in \mathbb{Z}^+$ definimos $a \cdot b = \underbrace{a + \ldots + a}_{b \text{ parcelas}}$.*
3. *se $a \in \mathbb{Z}^-$ e $b \in \mathbb{Z}^-$ definimos $a \cdot b = (-a) \cdot (-b)$.*

Com a definição 1.20 podemos recuperar facilmente as propriedades da multiplicação assim como a regra dos sinais para a multiplicação que listamos a seguir.

Propriedades 1.5 (Propriedades das multiplicação em $\mathbb{Z}$)**.**

1. Associativa: Para todo a, b e c números inteiros tem-se

$$(a \cdot b) \cdot c = a \cdot (b \cdot c);$$

2. Existência de Neutro: O número 1 é o único inteiro que verifica que

$$a \cdot 1 = a \quad \text{para todo } a \in \mathbb{Z}.$$

3. Existência de Inverso: Para cada número inteiro a existe um número inteiro simétrico com respeito à multiplicação, $a' \neq 0$, que chamamos de inverso de a verificando

$$a \cdot a' = 1. \tag{1.20}$$

4. Distributiva da multiplicação com respeito à adição:, propriedade que liga as operações de adição e multiplicação, que afirma

   $a \cdot (b + c) = a \cdot b + a \cdot c$, para todo $a,\ b$ e c inteiro.

5. Regra dos Sinais:

   - se $a \in \mathbb{Z}^+$ e $b \in \mathbb{Z}^+$ então $a \cdot b \in \mathbb{Z}^+$;
   - se $a \in \mathbb{Z}^+$ e $b \in \mathbb{Z}^-$ então $a \cdot b \in \mathbb{Z}^-$;
   - se $a \in \mathbb{Z}^-$ e $b \in \mathbb{Z}^-$ então $a \cdot b \in \mathbb{Z}^+$.

1.5 Múltiplos e divisores.

O que entendemos por *divisão* é a operação que permite averiguar quantas vezes um número, que denominamos **divisor** está contido em outro número, que chamamos de **dividendo**. Por exemplo, o número 3 está 4 vezes no número 12 já que, como vimos na multiplicação de números naturais, temos $3 \cdot 4 = 12$. Assim, podemos dizer que 12 dividido por 3 é igual a 4. Neste sentido, a operação inversa da multiplicação é a divisão, assim como da adição é a subtração. No caso desta operação temos que para cada par de números inteiros o resultado de subtrair é um número inteiro. Isto não acontece com a operação de divisão desde que não todo número inteiro pode ser expresso com produto de outros dois números inteiros: por exemplo o caso de dividir um barra de chocolate com 12 quadrados entre 5 pessoas. Teríamos que distribuir dois quadrados para cada pessoa e "sobrariam" dois quadrados. Veremos que isto é um problema de **divisibilidade** Em princípio iremos estudar quais são os critérios para determinar quais números inteiros podem ser "divididos" e quais não têm essa caraterística. Começamos com uma definição.

Definição 1.21. *A notação $d \mid n$ significa que existe um número inteiro k tal que $n = d \cdot k$. A notação $d \nmid n$ significa que $d \mid n$ é uma proposição falsa.*
A notação $d \mid n$ pode ser expressa das seguintes maneiras:

d *divide a* n*;*
d *é um divisor de* n*;*
d *é um fator de* n*;*
n *é um multiplo de* d*.*

Exemplo 1.14. Vamos ler as seguintes afirmações em forma equivalente:

$5 \mid 10$;
5 divide a 10;
5 é um divisor de 10;
5 é um fator de 10;
10 é multiplo de 5.

Exemplo 1.15. Temos que $5 \times 7 = 35$, logo temos que $5 \mid 35$ e que $7 \mid 35$. Podemos colocar em um conjunto todos os divisores 35, que é dado por

$$\{\pm 1, \pm 5, \pm 7, \pm 35\},$$

assim como podemos definir um conjunto de todos os múltiplos de 5

$$\{\ldots, -10, -5, 0, 5, 10, \ldots\}.$$

Note a diferença entre os conjuntos de divisores e múltiplos de um número inteiro: o primeiro é *finito* enquanto que o dos múltiplos é *infinito*. A primeira afirmação está enunciada na seguinte proposição.

Proposição 1.11. *Se d e n são números inteiros tal que $d \mid n$ e $n \neq 0$ então $|d| \leq |n|$.*

Demonstração: Da definição 1.21 temos que existe q inteiro tal que $n = q \cdot d$. Como $n \neq 0$ devemos ter $|q| \geq 1$ e pela monotonia da relação de ordem obtemos que $|n| = |q \cdot d| \geq |d|$. ■

Desafio!

Determine o conjunto dos divisores dos números 14, -6, 13 e 6. Denote esses conjuntos como $D(14)$, $D(-6)$, $D(13)$ e $D(6)$, respectivamente.
Anote observações que possa concluir destes conjuntos.

Clique aqui para ver a resposta.

Notação 1.3. Denotamos o conjunto dos divisores de a como $D(a)$ e denotamos o conjunto dos múltiplos de a como $M(a)$.

Algumas outras propriedades imediatas da definição são as seguintes:

Propriedades 1.6.

1. $1 \mid n$, ou seja, 1 divide todos os números inteiros.
2. Se $n \mid 1$ se e somente se $n = \pm 1$, ou seja, 1 e -1 são os únicos divisores de 1.
3. $d \mid 0$, ou seja, todos os números inteiros são divisores de 0.
4. $n \mid n$ isto é, todo inteiro é divisor de si mesmo.

Observação 1.12. As próximas observações e reflexões são muito importantes para sua formação. Preste bem atenção aos próximos **Pare e Pense**!

Sempre nos dizeram que a divisão por 0 não é possível. Já parou para pensar porque realmente?

De fato, no conjunto dos ***NÚMEROS REAIS*** a divisão por 0, como *operação binária* (veja definição 1.11), ***NÃO É POSSIVEL***.

A razão é por causa da *definição* da *operação inversa* do produto, *a divisão*, que afirma que

$$\frac{a}{b} = c \text{ se e somente se } a = b \cdot c,$$

sendo c o ***ÚNICO*** resultado. Isto como consequência que a divisão no conjunto dos números reais é uma operação binária!.

Assim, se tivermos que $\frac{a}{0} = b$ com a diferente de 0, isto não faria sentido, de acordo com a definição acima, pois se fosse verdade, teríamos que $a = 0 \cdot b$, o que não é verdade para $a \neq 0$.

Porém, a expressão $\frac{0}{0} = c$, teria sentido, por definição, pois $0 = 0 \cdot c = 0$, o que é verdade para todo c.

Então qual é o problema de dividir 0 entre 0 no conjunto dos números reais?

Lembre! gostaríamos de definir a divisão no conjunto dos números reais como uma operação

binária, inversa da multiplicação. Portanto o resultado de $\frac{0}{0}$ deveria ser único. Mas!, poderia ser que $\frac{0}{0} = 1$ ou $\frac{0}{0} = \pi$, já que ambas as expressões verificam a definição.

Então não podemos dividir 0 entre 0 por causa da falta de unicidade do resultado. Isto dentro do conjunto dos ***NÚMEROS REAIS***.

Então o mesmo ocorre no conjunto dos números inteiros e a definição de divisor de um número?

NÃO!... aqui estamos em um mundo diferente. A definição de ***DIVISOR*** de um número no conjunto dos ***NÚMEROS INTEIROS*** disse que um número inteiro a é divisor de um número inteiro b se ***EXISTIR***, não precisa ser único, um número inteiro c tal que $b = a \cdot c$.

E agora? no conjunto dos números inteiros e com a definição de divisor 1.21, que acabamos de revisar no parágrafo anterior, quais seriam os números inteiros que tem como divisor o número inteiro 0?

De acordo com a definição 1.21, no conjunto dos números inteiros, 0 vai ser divisor de b se e somente se existir ***ALGUM*** número inteiro c tal que $b = 0 \cdot c$. Note que, a única forma dessa igualdade ser certa é que $b = 0$. Logo...

Reflita sobre a conclusão e não leve um choque!: o único número ***DIVISOR INTEIRO*** de 0 é o número 0!!

Mais uma reflexão: esta propriedade é única do conjunto dos número inteiros. Mas!, veremos que existem conjuntos com divisores de 0, os quais iremos estudar no no módulo II.

Propriedades 1.7 (Propriedades do divisor e do múltiplo)**.** *Sejam $n,\ m,\ a,\ b$ e d inteiros. Então temos as seguintes propriedades da relação "divisor de":*

1. $d \mid n$ *e* $n \mid m$ *se e somente se* $d \mid m$*, que é a propriedade transitiva da relação "divisor de";*
2. $d \mid n$ *e* $d \mid m$ *então* $d \mid (n+m)$ *e* $d \mid n \cdot m$*;*
3. $(ad) \mid (an)$ *e* $a \neq 0$ *então* $d \mid n$ *que é propriedade de cancelamento;*
4. $d \mid n$ *e* $d \mid m$ *então* $d \mid an + bm$ *que é a propriedade de linearidade da relação "divisor de".*

Demonstração:

1. da hipótese e da definição 1.21 temos que existem k e l tais que $n = dk$ e $m = nl$ de onde obtemos que $m = (dk)l = d(kl)$. Ou seja, existe $r = kl$ inteiro tal que $m = dr$. Isto prova que $d \mid m$.

2. temos que existem k e l tais que $n = dk$ e $m = dl$, de onde $m + n = d(k + l)$ e $mn = d(kl)$. Isto demonstra a afirmação.

3. temos que $an = (ad)k$ para algum k inteiro e por hipótese $a \neq 0$ então, cancelando a se obtém $n = dk$, que mostra que $d \mid n$.

4. de que $d \mid n$ e $d \mid m$ pelo ítem 2, usando a propriedade do produto obtemos que $d \mid an$ e $d \mid bm$ e usando novamente o item 2 com a soma concluimos que $d \mid an + bm$.

■

Uma consequência do item 2 das propriedades 1.6 é o seguinte corolário que iremos usar na próxima seção 1.7.

Corolário 1.1. *Se* $d \mid a$ *então* $-d \mid a$*.*

Demonstração: se $d \mid a$ então $a = kd$ para algum inteiro k. Assim temos que $a = (-k)(-d)$. Como os números $-d$ e $-k$ são números inteiros, então, pela definição 1.21, obtemos que $-d \mid a$. ■

Definição 1.22. *Sejam os números inteiros a, b e c. Diz-se que c é uma combinação linear de a e b se existirem inteiros s e t tal que $c = as + bt$.*

Exemplo 1.16. O número inteiro 26 é uma combinação linear de 6 e 10 porque

$$26 = 2 \cdot 10 + 1 \cdot 6.$$

Não é tão claro que o número 4 é uma combinação linear de 6 e 10. De fato, veja que

$$4 = 4 \cdot 6 + (-2) \cdot 10.$$

Os números inteiros que são usados para construir a combinação linear chamam-se coeficientes dessa combinação linear.

Os coeficientes de uma combinação linear de inteiros de um número z sempre existem? São únicos? Em outras palavras, os coeficientes 4 e -2 que foram usados para obter 4 no exemplo 1.16 são os únicos com essa propriedade?
Esta pergunta será respondida na seção 1.8.

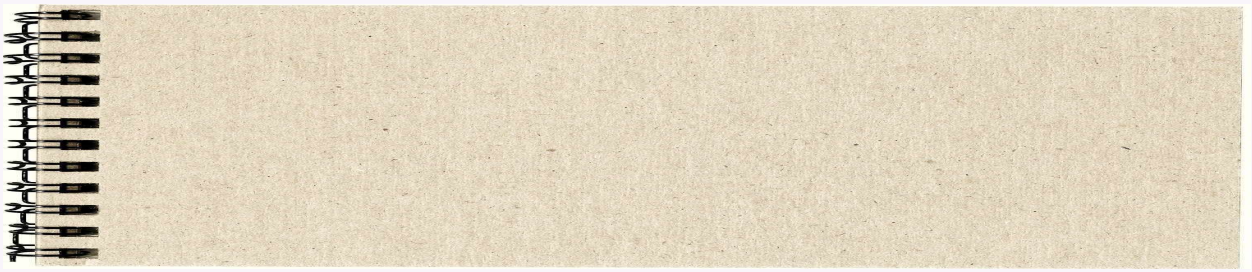
A resposta depende de que o problema $6 \cdot a + 10 \cdot b$ tenha solução inteira e ainda é preciso analisar se essa solução é única. Estudaremos estas questões ainda neste módulo.

Para usar nos exercícios propostos, precisaremos das seguintes definições, com as quais imaginamos que você deve estar bem familiarizado.

Definição 1.23. *Um inteiro n é dito par se existir um inteiro k tal que $n = 2 \cdot k$.*
Um inteiro m é dito ímpar se existir um inteiro h tal que $n = 2 \cdot h + 1$.
Chamamos de paridade de um inteiro a propriedade de ser par ou ímpar. Dois inteiros têm a mesma paridade se ambos são pares ou ímpares.

Desafio!

Mostre que 2 pode ser escrito como combinação linear de 6 e 10. A partir disso, mostre que todo número par pode ser expresso como combinação linear de 6 e 10. Anote suas conclusões no caderno.



Clique aqui para ver a resposta.

1.6 O Algoritmo da Divisão

Como explicado no começo desta seção, vamos definir para os casos em que o número inteiro a não seja múltiplo de d ou d não seja divisor de a um **operador** de $\mathbb{Z} \times \mathbb{Z}$ em $\mathbb{Z} \times \mathbb{Z}^+$ tal que a cada par de números inteiros (a, d), dividendo a e divisor d, faz corresponder um único par de inteiros (q, r), quociente q e resto r não negativo de forma que

$$\begin{array}{ccccccc} \text{dividendo} & = & \text{quociente} & \cdot & \text{divisor} & + & \text{resto} \\ a & = & q & \cdot & d & + & r \end{array}$$

A imagem deste operador é chamada de resultado da divisão inteira entre a e d. A forma prática de obter o quociente e resto da divisão de dois números inteiros é usando um procedimento que é conhecido como algoritmo da divisão inteira. Assim, o objetivo desta seção é estudar o seguinte teorema.

Teorema 1.2 (O Algoritmo da Divisão)**.** *Se a e b são inteiros e $b > 0$ então existem inteiros q e r satisfazendo as seguintes condições:*

$$a = bq + r \text{ e } 0 \leq r < b. \tag{1.21}$$

Além disso se existirem outros inteiros q_1 e r_1 verificando as condições (1.21)*, então*

$$q = q_1 \quad \text{e} \quad r = r_1, \text{ (unicidade).}$$

Demonstração: Seja $b > 0$ e a números inteiros dados. Temos duas possibilidades:

1. b divide a a e daí existe um número inteiro q talq eu $a = bq + 0$. Neste caso temos $r = 0$ e como $b > 0$, então a unicidade de q está garantida.

2. b não divide a a. Neste caso definimos o conjunto S como sendo

$$S = \{s = a - bt,\ t \in \mathbb{Z}, s \geq 0\}. \tag{1.22}$$

A primeira observação que fazemos é que, da definição do conjunto S, concluimos que é um conjunto de inteiros positivos. Portanto $S \subset \mathbb{N}$.

Uma segunda observação é que, se tomarmos $t_1 = -|a|$, então o elemento $s_1 = a - bt_1$ pertence ao conjunto S. De fato, temos que

$$s_1 = a - bt_1 = a - b(-|a|) = a + b|a| \geq a + |a|,$$

esta última desigualdade fundamentada em que $b > 0$ e portanto temos $b \geq 1$. Assim, usando a propriedade do módulo, temos que $s_1 \geq 0$.

Isto mostra que o conjunto S não é vazio e é um subconjunto de números naturais. Assim, pelo Princípio da Boa Ordenação (veja 1.1, pg. 39), deve existir r número natural mínimo de S.

Do fato de r ser mínimo de S, r pertence a S e portanto tem que existir $q \in \mathbb{Z}$ tal que

$$r = a - bq, \quad \text{de onde} \quad a = bq + r.$$

Resta provar que $0 < r < b$. Vamos supor que

$$r \geq b, \tag{1.23}$$

tentando chegar a uma contradição. Como $r = a - bq \geq b$ então devemos ter $a - bq - b \geq 0$. Portanto, o elemento

$$s_2 = a - bq - b = a - b(q + 1)$$

pertence ao conjunto S para o valor de $t = q + 1$. Usando novamente que r é o mínimo do conjunto S, deve verificar-se que

$$r \leq a - b(q + 1) = r - b \quad \text{de onde concluimos} \quad r \leq r - b \quad \text{ou seja} \quad b \leq 0,$$

o que é falso por hipótese! Assim, supor que (1.23) é verdadeira nos leva a uma contradição. Como consequência $r < b$ é verdadeiro.

A unicidade do quociente q e do resto, neste caso, r se mostra supondo que existem q_1 e r_1, outro quociente e resto, respectivamente, da divisão inteira de a por b. Assim, pela definição (1.21), temos que

$$a = bq_1 + r_1 \quad \text{e} \quad 0 < r_1 < b, \tag{1.24}$$

e também que

$$a = bq + r \quad \text{e} \quad 0 < r < b. \tag{1.25}$$

Vamos supor que $r_1 \neq r$, por exemplo que $r > r_1$. Subtraindo a equação (1.24) da equação (1.25) obtém-se

$$0 = a - a = (bq_1 + r_1) - (bq + r) = b(q_1 - q) + (r_1 - r).$$

Portanto, obtemos que

$$r - r_1 = b(q_1 - q). \tag{1.26}$$

Isto que implica que $b \mid r - r_1$. Pela proposição 1.11 temos que $b \leq r - r_1$. Por outro lado temos que

$$0 < r_1 < r < b,$$

ou seja, se verifica que $r - r_1 < b$, o que contradiz que $b \leq r - r_1$.

Supondo a outra desigualdade $r_1 > r$ chegaríamos da mesma maneira a uma contradição. Portanto devemos ter $r_1 = r$.

Finalmente, de (1.26) obtemos que $0 = b(q_1 - q)$. Como $b > 0$ devemos concluir que $q_1 - q = 0$, ou seja, $q_1 = q$, completando a demonstração do teorema. ■

Agora que temos certeza teoricamente da existência e unicidade do quociente e do resto de uma divisão inteira, como fazemos na prática para achá-los?

Para efetuar a divisão entre números naturais seguiremos o procedimento que aprendemos na escola. Recordemos que a forma gráfica de fazer a divisão de 345 por 13 é como segue

$$\begin{array}{r|l} 345 & 13 \\ \hline 7 & 26 \end{array}$$

de onde escrevemos que

$$345 = 26 \cdot 13 + 7. \tag{1.27}$$

E se queremos dividir por um número inteiro negativo? Isso parece uma novidade!

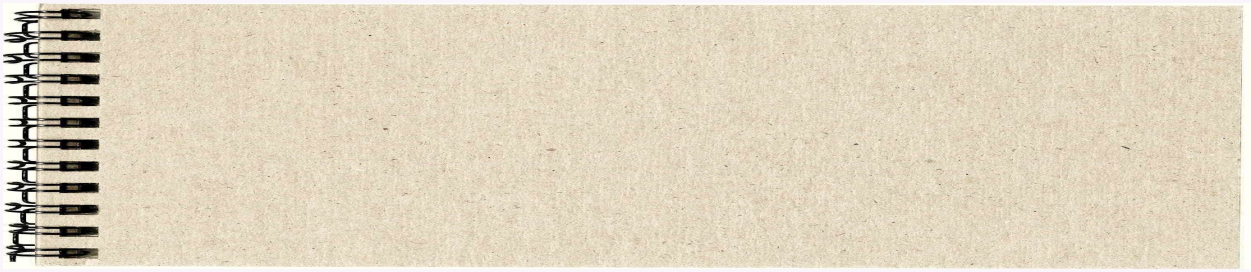
Por exemplo, se queremos saber o quociente e o resto da divisão inteira de 345 por -13, vamos aproveitar o resultado obtido em (1.27) da seguinte maneira

$$345 = (-1)26 \cdot (-1)13 + 7,$$

sendo então o quociente de dividir 345 por -13 o número inteiro -26 e resto 7. Compreendeu a "mágica"? Então vamos praticar.

Desafio!

Ache o quociente e resto da divisão inteira de 1.678 por -75. Anote o resultado no caderno.



Clique aqui para ver a resposta.

Ok! a questão do divisor ser um inteiro negativo foi resolvida. Agora a questão é ... e se o dividendo for um número inteiro negativo?

Vamos resolver essa questão também. Suponha que queremos dividir -345 por 13. De novo aproveitamos o resultado da divisão inteira de 345 por 13 e manipulamos este resultado como segue

$$-345 = -(26 \cdot 13 + 7) = (-26) \cdot 13 - 7, \tag{1.28}$$

só que o resto deve ser um número não negativo, portanto -7 não é o candidato a resto. A forma de resolver isto é somar e subtrair o divisor 13 ao segundo membro da igualdade (1.28), obtendo

$$-345 = (-26) \cdot 13 - 7 + 13 - 13 = (-26 - 1) \cdot 13 + (-7 + 13) = (-27) \cdot 13 + 6,$$

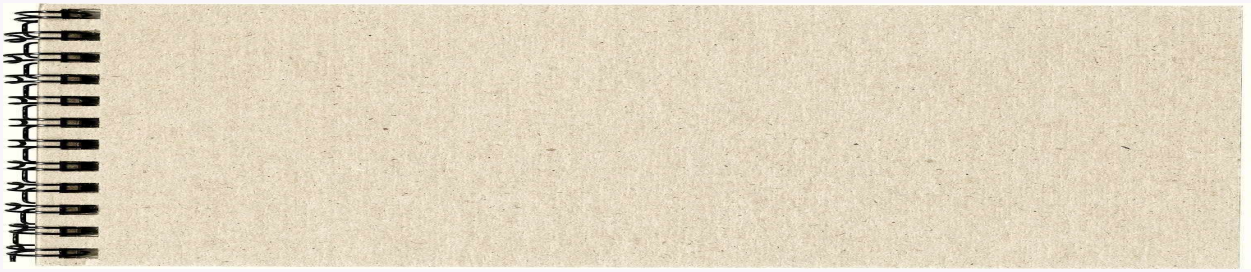
de onde concluimos pelo teorema 1.7 que $q = -27$ e $r = 6$.

Prezado aluno: você já imagina como responder à questão de uma divisão inteira com dividendo e divisor negativos? Tente no próximo desafio!

Desafio!

Resolva a questão proposta acima com os números -345 e -13.
Para praticar ache quociente e resto das seguintes divisões inteiras:

1. -2.311 dividido por -111;
2. -37 dividido por -5.



Clique aqui para ver a resposta.

Observação 1.13. O algoritmo da divisão inteira tem uma interessante aplicação na **representação dos números em diferentes bases** Lembre que todo número inteiro positivo pode ser escrito de uma única maneira como soma de produtos de *dígitos* multiplicados por potências de um número dado chamado de base. Os dígitos são os números naturais menores a essa base. A mais comum é a base 10, cujos dígitos pertencem ao conjunto $\{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9\}$.
Existem outras bases importantes, como é a base 2, que é a essência da linguagem computacional.

A seguir mostraremos o teorema que afirma a existência da representação de um número em qualquer base. Isto você já viu no curso de Matemática Elementar. Iremos então revisar estas ideias com alguns exemplos de como converter um número expresso em uma base dada para outra base.

Teorema 1.3. *Seja b um número inteiro maior do que 1. Então qualquer outro número inteiro positivo pode ser expresso de uma única maneira como*

$$m = a_l b^l + a_{l-1} b^{l-1} + ... + a_1 b + a_0, \tag{1.29}$$

onde $l > 0$ inteiro, $0 \leq a_j < b$ para $j = 0, 1, ..., l$ e $a_l \neq 0$.

Demonstração: *Efetuamos a divisão inteira de m por b obtendo*

$$m = bq_0 + a_0, \quad 0 \leq a_0 < b. \tag{1.30}$$

No caso que $q_0 \neq 0$, dividimos q_0 por b obtendo

$$q_0 = bq_1 + a_1, \quad 0 \leq a_1 < b. \tag{1.31}$$

Continuando este processo temos que

$$\begin{array}{rcl} q_1 & = & bq_2 + a_2, \quad 0 \leq a_2 < b, \\ & \vdots & \\ q_{l-2} & = & bq_{l-1} + a_{l-1}, \quad 0 \leq a_{l-1} < b, \\ q_{l-1} & = & b \cdot 0 + a_l, \quad 0 \leq a_l < b. \end{array}$$

Note que a sequência de números $q_0, q_1, \ldots$ é decrescente, isto é, $q_0 > q_1 > \ldots$, de forma que o quociente da última divisão deve ser o número 0. Substitutindo na equação em (1.30) *q_0 pela expressão dada na equação* (1.29)*, obtém-se*

$$m = b(bq_1 + a_1) + a_0 = b^2 q_1 + a_1 b + a_0,$$

e, continuando a substituir, chegamos a que

$$\begin{array}{rcl} m & = & b^3 q_2 + a_2 b^2 + a_1 b + a_0, \\ & \vdots & \\ & = & b^l q_{l-1} + a_{l-1} b^{l-1} + ... + a_1 b + a_0, \\ & = & a_l b^l + a_{l-1} b^{l-1} + ... + a_1 b + a_0, \end{array}$$

que é a expressão em (1.30)*. Falta provar a unicidade desta expressão. Suponha que exista outra forma de expressar m na base b. Então teríamos*

$$m = a_l b^l + a_{l-1} b^{l-1} + ... + a_1 b + a_0 = c_l b^l + c_{l-1} b^{l-1} + ... + c_1 b + c_0, \tag{1.32}$$

onde, se o numero de termos é diferente completamos com zeros para fazer que as duas expressões tenham o mesmo número de termos. De (1.32) *concluimos que*

$$(a_l - c_l) b^l + (a_{l-1} - c_{l-1}) b^{l-1} + ... + (a_1 - c_1) b + (a_0 - c_0) = 0.$$

Supondo que as expressões são diferentes então deve existir algum $0 \leq j \leq l$ *tal que* $c_j \neq a_j$ *e como consequência temos*

$$b^j((a_l - c_l)b^{l-j} + \cdots + (a_{j+1} - c_{j+1})b + (a_j - c_j)) = 0.$$

Do fato que $b \neq 0$*, obtemos que*

$$(a_l - c_l)b^{l-j} + \cdots + (a_{j+1} - c_{j+1})b + (a_j - c_j) = 0.$$

Por outro lado,

$$c_j - a_j = (a_l - c_l)b^{l-j} + \cdots + (a_{j+1} - c_{j+1})b,$$

e como resultado obtemos que $b \mid (a_j - c_j)$*. Como* $0 \leq a_j < b$ *e* $0 \leq c_j < b$*, chegamos à conclusão de que* $a_j = c_j$*, o que é um absurdo. Isto demonstrou a unicidade da representação.* ■

Exemplo 1.17. Para converter a representação decimal de 214 para a base 3:

$$\begin{aligned} 214 &= 3 \cdot 71 + 1 \\ 71 &= 3 \cdot 23 + 2 \\ 23 &= 3 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \\ 2 &= 3 \cdot 0 + 2 \end{aligned}$$

Assim, tomando os restos das divisões inteiras na ordem da última divisão até a primeira, obtemos que $(214)_{10} = (21221)_3$.

1.7 Máximo Divisor Comum

Além de conhecer os divisores de um número inteiro, pode ser útil de saber calcular, como na época da escola, os divisores em comum de dois ou mais inteiros e então achar o maior de todos eles. Por exemplo, sabemos que os divisores 36 são os elementos do conjunto

$$D(36) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 9, \pm 12, \pm 18, \pm 36\}.$$

Também sabemos que os divisores de 45 são

$$D(45) = \{\pm 1, \pm 3, \pm 5, \pm 9, \pm 15, \pm 45\}.$$

Assim vemos que os números que pertencem a ambos os conjuntos, ou seja, a interseção de $D(36)$ com $D(45)$, são os divisores em comum de 36 e 45. Portanto,

$$D(36) \cap D(45) = \{\pm 1, \pm 3, \pm 9\}.$$

Também observamos que o maior comum divisor é 9.

Vamos fazer a seguir a definição formal destes conceitos.

Definição 1.24. *Dados os números inteiros $a,\ b$ e d, se $d \mid a$ e $d \mid b$ dizemos que d é divisor comum de a e b.*

Notação 1.4. O conjunto formado pelos divisores comuns de a e b é denotado por $D(a,b)$. Temos então

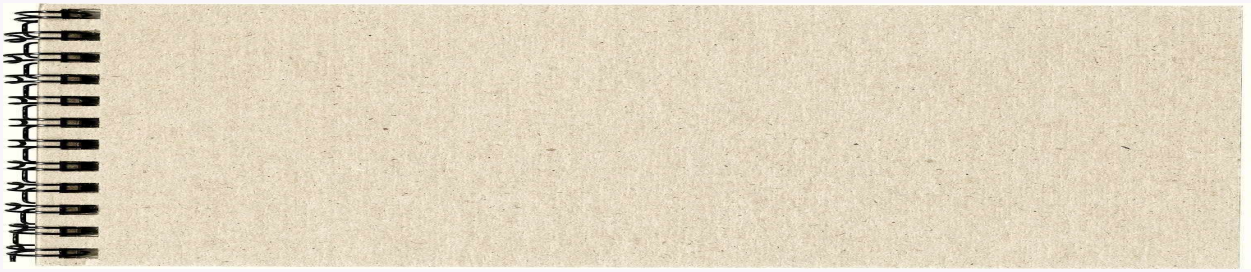
$$D(a,b) = D(a) \cap D(b) = \{d :\ d \mid a \text{ e } d \mid b\}.$$

Observe que como 0 é divisível por qualquer número inteiro, então temos que $D(0,0) = \mathbb{Z}$, de onde o conjunto $D(0,0)$ não possui máximo elemento. Porém, se $a \neq 0$ ou $b \neq 0$, podemos encontrar o máximo do conjunto $D(a,b)$. Assim, podemos fazer a definição 1.25.

Definição 1.25. *Dados $a, b \in \mathbb{Z}$, se $a \neq 0$ ou $b \neq 0$, definimos como Máximo Divisor Comum e denotamos por $\mathrm{MDC}(a,b)$ ao maior inteiro d que divida a a e b. Por questões técnicas, definimos $\mathrm{MDC}(0,0) = 0$.*

Desafio!

Usando estritamente a definição 1.25, como no exemplo inicial, ache o maior divisor comum de -18 e 30. Faça o mesmo desafio para -12 e -36. Anote os resultados no caderno.



Clique aqui para ver a resposta.

Observação 1.14. *Podemos também generalizar o conceito de* MDC *para vários números, utilizando a interseção dos três conjuntos de divisores*

$$D(12, 24, 54) = \{\pm 1, \pm 2, \pm 3, \pm 6\},$$

de onde o maior divisor comum de $12,\ 24$ *e* 54 *é* 6.

Tinhamos já observado que o conjunto dos divisores de um número inteiro é um **conjunto finito**. Verificaremos esta ideia no próximo lema.

Lema 1.1. *Seja* $a \neq 0$. *Então o maior número positivo que divide* a *é* $|a|$.

Demonstração: Note que $|a|$ divide a. De fato, se $a > 0$ e do fato que $a \mid a$ temos que $|a| \mid a$. No caso que $a < 0$ então temos $|a| = -a$ e daí

$$a = (-a)(-1) = |a|(-1),$$

o que mostra que $|a|$ é um fator de a. Em qualquer dos dois casos, temos que $|a|$ divide a e ambos os casos temos que $|a| > 0$ porque $a \neq 0$.

Supondo agora que $d \mid a$ e d é positivo, então temos que $a = dk$ para algum inteiro k. Portanto $-a = d(-k)$, o que implica que $d \mid |a|$. Pela proposição 1.7 concluímos que $d \leq |a|$. ■

Os próximos lemas são afirmações sobre propriedades importantes do MDC de dois ou mais números inteiros.

Lema 1.2. *Dados dois números inteiros* a *e* b, *temos que*

$$\mathrm{MDC}(a, b) = \mathrm{MDC}(|a|, |b|).$$

Demonstração: Quando $a = 0$ e $b = 0$, temos $|a| = a$ e $|b| = b$. Assim temos que

$$\mathrm{MDC}(a, b) = \mathrm{MDC}(|a|, |b|).$$

Suponha agora que a ou b não são nulos. Observe que $d \mid a$ se e somente se $d \mid |a|$, de onde temos que

$$\mathrm{MDC}(a, b) = \mathrm{MDC}(|a|, |b|).$$

Portanto, o maior divisor comum de a e b coincide com maior divisor comum de $|a|$ e $|b|$. ■

Observe que o lema 1.2 mostra que o cálculo do MDC pode ser restrito a números inteiros positivos. Ou seja, do jeito que você ensina ou aprendeu na escola!

Lema 1.3. *Dados dois numeros inteiros a e b temos que* $\mathrm{MDC}(a, b) = \mathrm{MDC}(b, a)$.

Demonstração: Como os conjuntos $D(a, b)$ e $D(b, a)$ são iguais, então os máximos desses conjuntos coincidem. Isto completa a prova! ■

Note que o lema 1.3 se refere à comutatividade da relação MDC entre pares de números inteiros.

Finalmente, podemos enunciar e demonstrar teoricamente a existência do $\mathrm{MDC}(a, b)$ para qualquer par de inteiros $a \neq 0$ e $b \neq 0$.

Teorema 1.4. *Dados $a \neq 0$ e $b \neq 0$, então $\mathrm{MDC}(a, b)$ existe e satisfaz*

$$0 < \mathrm{MDC}(a, b) \leq \min\{|a|, |b|\}.$$

Demonstração: Lembre que o $\mathrm{MDC}(a, b)$ é o máximo do conjunto $D(a, b)$. Como $1 \mid a$ e $1 \mid b$ então temos que $1 \in D(a, b)$. Assim o máximo tem que ser maior que todo elemento de $D(a, b)$ e portanto maior que 1. Por outro lado, se $d \in D(a, b)$ então $d \mid |a|$ e $d \mid |b|$, de onde d não pode ser maior que $|a|$ e $|b|$. Isto nos leva à conclusão de que d é pelo menos menor que $|a|$ e $|b|$, obtendo que $\mathrm{MDC}(a, b) \leq \min\{|a|, |b|\}$. ■

Exemplo 1.18. Dos lemas 1.3-1.2 e do teorema 1.4, podemos afirmar que

$$\begin{aligned} \mathrm{MDC}(48, 732) &= \mathrm{MDC}(-48, 732) \\ &= \mathrm{MDC}(-48, -732) \\ &= \mathrm{MDC}(48, -732). \end{aligned}$$

assim como

$$0 < \mathrm{MDC}(48, 732) \leq 48.$$

Sendo $d = \mathrm{MDC}(48, 732)$, então $d \mid 48$ e para encontrar d precisamos somente checar os divisores positivos de 48 que também dividem 732.

A próxima afirmação será útil para a próxima seção 1.8.

Lema 1.4. *Seja a um número inteiro positivo. Então $\mathrm{MDC}(a, 0) = a$.*

Demonstração: Como todo número inteiro divide o 0, então temos que $D(a, 0)$ é o conjunto de divisores de a. Pelo lema 1.1 sabemos que o maior divisor de a é $|a|$. Logo, como temos $a > 0$ então $|a| = a$. Isto mostra que $\mathrm{MDC}(a, 0) = a$. ■

Para finalizar esta seção, iremos demonstrar alguns resultados que usaremos na seção 1.9. Entre eles uma proposição muito útil conhecida como a Identidade de Bézout. O matemático francês Étienne Bézout (1730-1783) não provou a identidade que leva seu nome mas um resultado análogo para polinômios. Foi Claude Gaspard Bachet de Méziriac (1581-1638), outro matemático francês, quem provou a identidade para números inteiros como conhecemos na atualidade como identidade de Bezout.

Teorema 1.5 (Identidade de Bézout)**.** *Sejam a e b inteiros positivos e $d = \mathrm{MDC}(a, b)$. Então existem inteiros m e n tal que $ma + nb = d$.*

Demonstração: (da Identidade de Bezout)

Seja o conjunto $A = \{x = ma + nb,\ x \in \mathbb{N}\}$. Este conjunto é um conjunto de números naturais não vazio. Então, pelo princípio da boa ordenação (veja no módulo 1, 1.1, pg. 39) existe x_0 o mínimo de A. Assim sabemos que x_0 é multiplo de d porque ambos, a e b, são múltiplos d. Queremos provar que $x_0 = d$. Suponha o contrário. Como d é o maior divisor comum entre a e b, se supormos $x_0 > d$ então x_0 não pode ser um divisor comum e portanto temos que $x_0 \nmid a$ ou $x_0 \nmid b$. Suponha que $x_0 \nmid a$. Obtemos da divisão inteira de a por x_0 que

$$\begin{array}{r|l} a & x_0 \\ r & q \end{array}, \quad \text{com } 0 \leq r < x_0.$$

Assim temos que $r = a - qx_0$, ou seja r é uma combinação linear de a e b. Ou seja, $r \in A$ e é menor que o mínimo de A. Isto e uma contradição. Fariamos a mesma prova supondo que $x \nmid b$. Logo devemos ter $x_0 = d$ e, como por ser mínimo $x_0 \in A$, obtemos que $d = x_0 = ma + nb$ para algum m e n inteiros. ■

O teorema de Bezout enuncia que o máximo divisor comum entre a e b pode ser sempre expresso como combinação linear destes números. Em particular, quando temos $\mathrm{MDC}(a, b) = 1$ vamos poder escrever $ma + nb = 1$ para algum m e n inteiros!

Definição 1.26. *Os números m e n da combinação linear $ma + nb = \mathrm{MDC}(a, b)$ são chamados de coeficientes de Bézout.*

Vamos a aprender a calcular esses coeficientes na seção 1.8. O próximo corolário 1.2 é a resposta à pergunta deixada para pensar na seção 1.5.

Corolário 1.2. *Sejam a e b dois inteiros não nulos. Então o número inteiro c é uma combinação linear de a b se e somente se c é um múltiplo do $\mathrm{MDC}(a, b)$.*

Como consequência da Identidade de Bézout temos um famoso resultado devido a Euclides. O matemático de Alexandria, Euclides (em torno de 325 AC - 265 AC), além de ser o pioneiro na formulação axiomática da geometria euclidiana, contribuiu com resultados importantes para a teoria dos números (inteiros). Veremos outro resultados de Euclides ao longo deste curso.

Proposição 1.12 (Lema de Euclides)**.** *Suponha que $a \mid bc$ e $\mathrm{MDC}(a, b) = 1$. Então $a \mid c$.*

Demonstração: Como $\mathrm{MDC}(a, b) = 1$, pela identidade de Bézout temos que existem s e t números inteiros, tais que $1 = as + bt$, de onde, multiplicando ambos os membros desta igualdade por c, obtém-se

$$c = cas + cbt = a(cs) + (bc)t.$$

Temos então que $a \mid bc$ e claramente que $a \mid a(cs)$ de onde deduzimos pela propriedade 1.7 que a divide a combinação linear $a(cs) + (bc)t = c$. ■

Definição 1.27. *Diz-se que* a *e* b *são* primos entre si *ou* coprimos *ou* relativamente primos *se* $\mathrm{MDC}(a, b) = 1$.

A partir da definição 1.27 podemos enunciar de outra forma a proposição 1.12 como segue:

Lema 1.5 (Lema de Euclides)**.** *se* $a \mid bc$ *e* a *é um número primo com* b*, então* $a \mid c$.

Observação 1.15. Em geral não é verdade que se $a \mid bc$ então $a \mid b$ ou $a \mid c$.
Um contraexemplo pode ser o seguinte: temos que $6 \mid 4 \cdot 9$ mas $6 \nmid 4$ e $6 \nmid 9$.
A razão pela qual o lema 1.5 não se aplica é pelo fato que temos $\mathrm{MDC}(6, 4) \neq 1$ e $\mathrm{MDC}(6, 9) \neq 1$.

Finalmente, uma generalização do lema de Euclides é o seguinte lema 1.6.

Lema 1.6. *Sejam* p*, um número primo, e* $a_1, \ldots, a_n,\ n > 1$*, números inteiros. Supondo* $p \mid a_1 \ldots a_n$*, então* $p \mid a_i$ *para algum* $i \in \{1, 2, \ldots, n\}$.

Demonstração: A demonstração é feita pelo princípio de indução a partir de $n = 2$, que é verdadeiro, pois não é outra coisa que o lema de Euclides 1.12.

Para $n > 2$ observe que

$$a_1 \ldots a_n = (a_1 \ldots a_{n-1})a_n.$$

Então, pelo Lema de Euclides temos que $p \mid a_1 \cdots a_{n-1}$ ou $p \mid a_n$. Acontecendo isto no último, o teorema fica provado. Caso que tenhamos $p \mid a_1 \cdots a_{n-1}$, pela hipótese indutiva temos que $p \mid a_i$ para algum $i \leq n - 1$. ■

1.8 O Algoritmo de Euclides

O **algoritmo** de Euclides fornece um método para achar o MDC de dois números inteiros. Como temos visto na seção 1.7, basta saber o MDC de números positivos desde que temos $\mathrm{MDC}(0, 0) = 0$, $\mathrm{MDC}(a, b) = \mathrm{MDC}(|a|, |b|)$ e $\mathrm{MDC}(a, b) = \mathrm{MDC}(b, a)$.

Lema 1.7. *Sejam* $b > a > 0$. *Se* $b = aq + r$ *então* $\mathrm{MDC}(a, b) = \mathrm{MDC}(a, r)$.

Demonstração. Como temos que $b = q \cdot a + r$ então todo divisor comum de a e r é também divisor de b.

Por outro lado, como $r = b - q \cdot a$, logo todo divisor comum de a e b é divisor de r.

Concluímos que os pares de números (a, b) e (a, r) têm exatamente os mesmos divisores e como consequência o mesmo MDC. □

Mostraremos com um exemplo como é que funciona o algoritmo de Euclides a partir da demonstração do lema 1.7.

Exemplo 1.19. Vamos calcular $\mathrm{MDC}(803, 154)$.

$$\begin{array}{rcll} \mathrm{MDC}(803,154) & = & \mathrm{MDC}(154,33) & \text{porque} \quad 803 = 154 \cdot 5 + 33 \\ \mathrm{MDC}(154,33) & = & \mathrm{MDC}(33,22) & \text{porque} \quad 154 = 33 \cdot 4 + 22 \\ \mathrm{MDC}(33,22) & = & \mathrm{MDC}(22,11) & \text{porque} \quad 33 = 22 \cdot 1 + 11 \\ \mathrm{MDC}(22,11) & = & \mathrm{MDC}(11,0) & \text{porque} \quad 22 = 11 \cdot 2 + 0 \\ \mathrm{MDC}(11,0) & = & 11 & . \end{array}$$

Portanto $\mathrm{MDC}(803, 154) = 11$.

Observação 1.16. *Observe que obtivemos o* MDC *de* 803 *e* 154 *sem usar fatoração em números primos. Este método é muito mais rápido, especialmente porque fatorar é uma tarefa dificil.*

Uma forma esquemática de fazer o algoritmo de Euclides é descrita a seguir. Primeiramente dividimos 803 por 154 e colocamos na seguinte tabela:

	5
803	**154**
33	

colocando o quociente 5 na primeira linha da segunda coluna e o resto na terceira linha da primeira coluna.

Dividimos 154 por 33, seguindo o algoritmo, estendendo a tabela de maneira que o quociente 4 fique na primeira linha da terceira coluna e o resto 22 na terceira linha da segunda coluna, como mostra a tabela:

	5	4
803	154	33
33	22	

Seguindo esse processo transportamos o número 22 para a segunda linha, que é a linha dos divisores, como mostra a seguinte tabela:

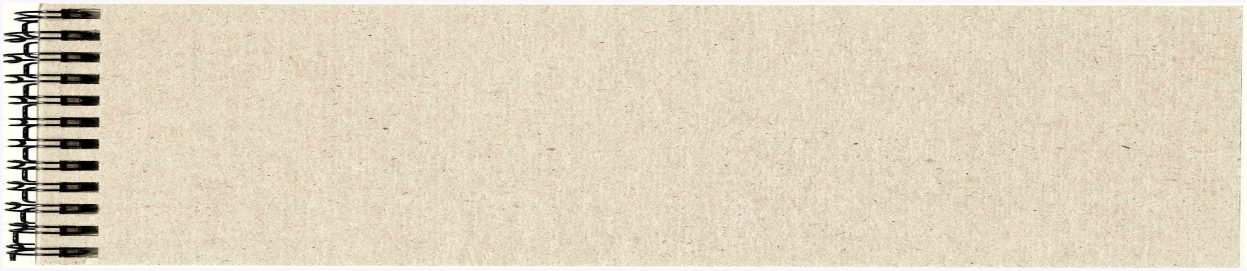
	5	4	1
803	154	33	22
33	22	11	

Seguindo esse processo até chegar a obter o resto 0. Então o último divisor que ocupa a segunda linha será o MDC de 803 e 154 como mostra a tabela:

	5	4	1	2	
803	154	33	22	11	$=\mathrm{MDC}(803, 154)$
33	22	11	0		

Desafio!

Calcule $\mathrm{MDC}(456, 203)$ e $\mathrm{MDC}(5.560, 3.535)$ usando o algoritmo de Euclides. Anote o resultado no caderno.



Clique aqui para ver a resposta.

Outra forma de computar o MDC de dois números é usando outra versão do algoritmo de Euclides, onde a divisão inteira não é a base do algoritmo. Este outro método é baseado na seguinte proposição.

Lema 1.8. *Se a e b não são nulos simultaneamente então*

$$\mathrm{MDC}(a,b) = \mathrm{MDC}(a, b-a).$$

Demonstração: Temos que um divisor de a e b é também divisor de $b-a$. Como temos $b = a + (b-a)$ então um divisor de a e $b-a$ é também divisor de b. Concluímos que os pares (a,b) e $(a, b-a)$ têm exatamente os mesmos divisores e, como consequência, o mesmo MDC. ■

Esta versão do Algoritmo de Euclides consiste em repetir o raciocínio do lema 1.8.

Exemplo 1.20. Vamos encontrar o $\mathrm{MDC}(90, 126)$ usando sucessivamente o lemalemaversao2 .
Como 126-90=36 lema 1.8 nos diz que

$$\mathrm{MDC}(90, 126) \;=\; \mathrm{MDC}(90, 36).$$

Agora subtraindo 36 de 90, reduzimos o problema a:

$$\mathrm{MDC}(90, 36) \;=\; \mathrm{MDC}(54, 36).$$

Como 36 é o menor ainda, subtraimos de novo de 54 para obter:

$$\mathrm{MDC}(54, 36) \;=\; \mathrm{MDC}(18, 36).$$

Subtraindo 18 de 36, temos

$$\mathrm{MDC}(18, 36) \;=\; \mathrm{MDC}(18, 18) \;=\; 18.$$

Concluindo que $\mathrm{MDC}(90, 126) = 18$.

Podemos usar uma tabela similar à do algoritmo de Euclides para este novo algoritmo. Colocamos na segunda linha da primeira coluna a diferença entre 126 e 90. Essa diferença colocamos na primeira linha da terceira coluna e a seguir fazemos a diferença entre esse número e o da primeira linha da segunda coluna. Assim, sucessivamente, para obter a tabela:

126	90	36	54	18	36	18	18
36	54	18	36	18	18	0	

sendo o último elemento da primeira linha depois da diferença o resultado 0, que é o MDC procurado.

Vejamos outro exemplo deste algoritmo da diferença.

Exemplo 1.21. Vamos encontrar o $\mathrm{MDC}(42, 144)$.

144	42	102	60	42	18	24	6	18	12	6	6
102	60	42	18	24	6	18	12	6	6	0	

Logo, o número procurado é 6.

Uma questão a ser pensada seria a seguinte: qual é o mais rápido dos algoritmos de Euclides? o da divisão ou da diferença?

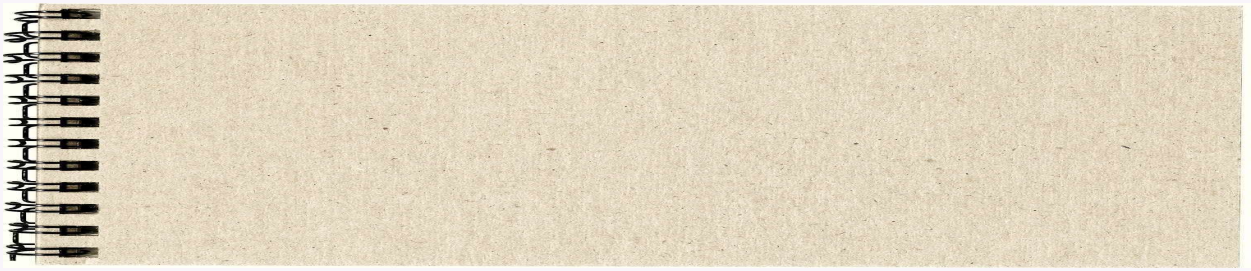
Note que a segunda forma do algoritmo de Euclides envolve subtrações repetidas. De fato, neste algoritmo temos um total 12 passos para chegar ao resultado. Assim, dividir é mais rápido, já que se reduz a quatro passos:

	3	2	6
144	**42**	18	3
18	6	**0**	

Uma propriedade importante do algoritmo de Euclides é que permite obter na prática os coeficientes de Bézout (veja na seção 1.7, 1.26, 67). Com efeito, note que cada resto que aparece no algoritmo de Euclides é uma combinação linear dos anteriores.

Desafio!

Calcule os coeficientes de Bézout dos números 37 e 13. Faça os cálculos no caderno.



Clique aqui para ver a resposta.

O processo de encontrar os coeficientes de Bézout é conhecido como **algoritmo estendido de Euclides**. Vejamos outro exemplo.

Exemplo 1.22. Encontre os números inteiros m e n tais que

$$m \cdot 62 + n \cdot 24 = 2.$$

Primeiramente executamos o algoritmo de Euclides:

	2	1	1	2	2
62	**24**	14	10	4	2
14	10	4	2	**0**	

A seguir expressamos os restos $14,\ 10,\ 4$ e 2 como diferenças:

$$\begin{aligned} 14 &= 62 - 2 \cdot 24 \\ 10 &= 24 - 1 \cdot 14 \\ 4 &= 14 - 1 \cdot 10 \\ 2 &= 10 - 2 \cdot 4 \end{aligned}$$

Continuando os cálculos de baixo para cima, obtemos

$$\begin{aligned} 2 &= 10 - 2 \cdot \overbrace{(14 - 1 \cdot 10)}^{4} \\ &= 3 \cdot 10 - 2 \cdot 14 \\ &= 3 \cdot \overbrace{(24 - 1 \cdot 14)}^{10} - 2 \cdot 14 \\ &= 3 \cdot 24 - 5 \cdot 14 \\ &= 3 \cdot 24 - 5 \overbrace{(62 - 2 \cdot 24)}^{14} \\ &= (-5) \cdot 62 + 13 \cdot 24, \end{aligned}$$

Logo, temos $m = -5$ e $n = 13$, que constituem os coeficientes de Bézout.

1.9 Números Primos

Estudaremos aqui um assunto que imaginamos que você manipulou bastante na escola e no colegio: é o conceito de número primo.

Estamos acostumados a trabalhar com números naturais. Por isso esta seção será dedicada aos inteiros positivos.

Definição 1.28. *Um número inteiro p é dito primo se possui exatamente quatro divisores que são $1,\ -1,\ -p$ e p.*
Um inteiro n é dito composto se n não é primo.

Da definição 1.28 vemos que o conjunto dos números inteiros é particionado em três conjuntos disjuntos cuja união é $\mathbb{Z}$, da seguinte forma:

$$\mathbb{Z} = \{\pm 1\} \cup \{z \in \mathbb{Z}, \quad \text{primo}\} \cup \{z \in \mathbb{Z}, \quad \text{composto}\}$$

Exemplo 1.23. O número 10 não é primo, pois pode ser dividido por $1,\ 2,\ 5$ e 10. O número 5 é primo, pois $D(5) = \{1,\ -1,\ -5,\ 5\}$.

- Os números ± 1 não são nem primos nem compostos!
- Os primeiros números primos positivos são:

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37...$$

- Note que o único número primo positivo que é *par* é o 2. Todos os restantes são ímpares.

Proposição 1.13. *Suponha que a é um número inteiro composto. Então existem b e c inteiros tais que $1 < |b| < a$ e $1 < |c| < a$ verificando $a = bc$.*

Demonstração: Sendo a composto, existe b número inteiro tal que $b \mid a$, de onde concluímos a existência de c tal que $a = cb$. Como c também é divisor de a, pela proposição 1.11 (veja seção 1.5, pg.51) temos que $1 < |b| < a$ e $1 < |c| < a$. ■

Observação 1.17. A proposição 1.13 ainda pode ser mais específica pois, do fato que $1 < |b| < a$ e $1 < |c| < a$, por monotonia temos que $1 < |bc| < a^2$. Portanto qualquer fator de a deve ser menor ou igual que $\sqrt{a}$.

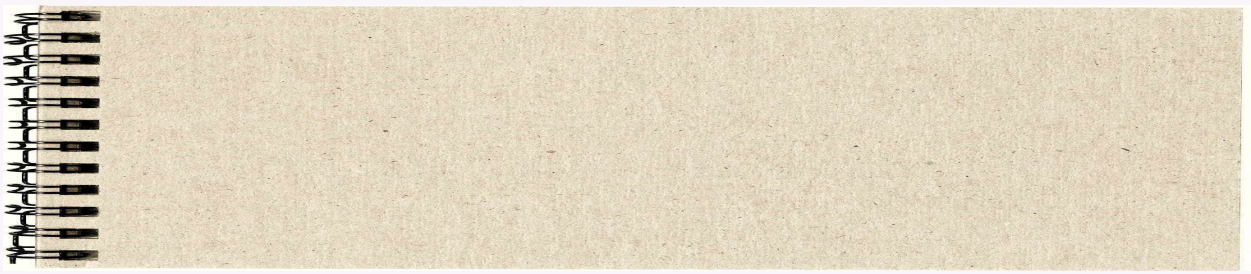
A observação 1.17 é muito útil para averiguar se um número inteiro é primo ou não. Por exemplo, os números do conjunto $A = \{109,\ 113,\ 127,\ 131,\ 137\}$ são primos. De fato, temos que $13^2 = 169$, sendo 169 maior que todos os números do conjunto A. Então, se os elementos do conjunto A tiveram mais algum divisor que ± 1 ou ele mesmo, ou seu oposto, teriam que ser do conjunto $\{2,\ 3,\ 5,\ 7,\ 11\}$ que são menores que 13. Com uma calculadora em mão, você pode verificar que nenhum dos números do conjunto B divide aos números do conjunto A. Portanto o conjunto A é um conjunto de números primos (exemplo extraído de Graña et al [10])

Desafio!

Comprovar que os números do conjunto

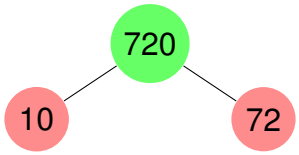
$$A = \{1.009,\ 1.013,\ 1.021,\ 1.031,\ 1.033,\ 1.039,\ 1.049,\ 1.051\}$$

são números primos.

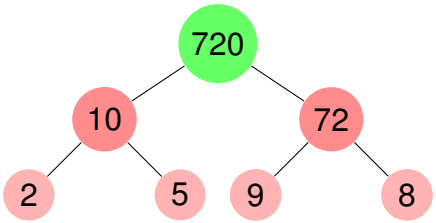


Clique aqui para ver a resposta.

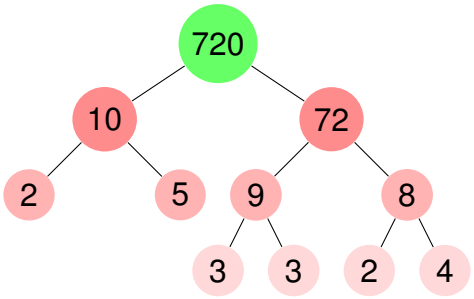
A proposição 1.13 se refere ao fato de que todo número composto pode ser fatorado e essa decomposição é chamada de fatoração do número a. Usando repetidamente a fatoração de números compostos, podemos expressar um número inteiro como produto de números primos. Vejamos um exemplo a seguir.



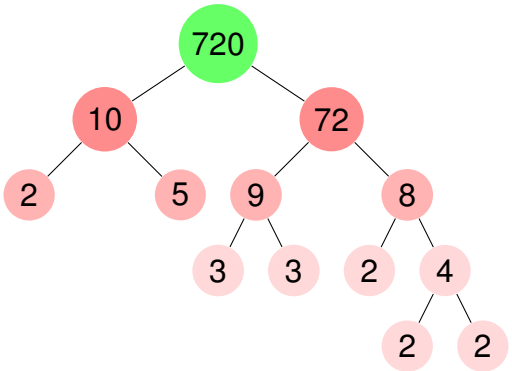
Vamos tomar o número 720, que é composto, e temos como fatoração inicial o produto de 10 por 72:



Como tanto 10 quanto 72 são ambos compostos, podemos fatorar esses números também, obtendo a seguinte árvore dos divisores de cada um dos fatores:



Ou seja, temos "quebrado" o número 720 em quatro fatores $2 \cdot 5 \cdot 9 \cdot 8$, cujo produto é 720. Dois desses fatores, 2 e 5, são primos. Os outros dois fatores, 9 e 8, ainda podem ser fatorados, obtendo

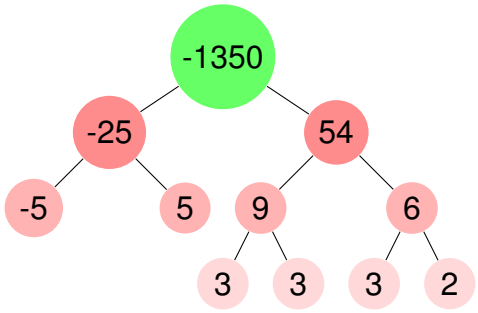


ou em forma de produto:

$$2 \cdot 5 \cdot 3 \cdot 3 \cdot 2 \cdot 2 \cdot 2 = 720.$$

Esta última expressão é que é chamada de fatoração por fatores primos de 720.

E a fatoração de um número inteiro negativo? Por exemplo -1350. Voltemos a fazer a árvore de fatores:



de onde obtemos que

$$-1350 = -5 \cdot 5 \cdot 3 \cdot 3 \cdot 3 \cdot 2 = (-1)5 \cdot 5 \cdot 3 \cdot 3 \cdot 3 \cdot 2,$$

que é o oposto da fatoração de 1350.

Isto pode ser feito com qualquer número composto. Como primeiro passo para demonstrar este fato, vamos mostrar que todo número inteiro possui pelo menos um divisor primo. Este fato é mais uma aplicação do princípio da boa ordenação (veja 1.4, teorema 1.1, pg. 39).

Proposição 1.14. *Se $a > 1$, existe um número primo p tal que $p \mid a$.*

Demonstração: Seja S o seguinte conjunto:

$$S = \{n : \ n > 1 \text{ e no possui um divisor primo}\}.$$

Se o conjunto S não fosse vazio, pelo princípio da boa ordenação, tem um mínimo, o qual chamaremos de m. Então $m > 1$ e não possui um divisor primo e pela definição 1.28, m tem que ser composto. Pela proposição 1.13 existem c e b inteiros positivos, verificando

$$m = bc, \quad 1 < b < m, \quad 1 < c < m.$$

Como $1 < b < m$ então b não está em S. Logo b tem que ter um divisor primo p. Como $p \mid b$ e $b \mid m$ pelo lema de Euclides (veja 1.7, a proposição 1.12, pg. 67) temos que $p \mid m$ que contradiz que m pertence a S. ■

A próxima proposição mostra que existem infinitos números primos. Mais uma afirmação devida ao Euclides de Alexandria.

Teorema 1.6 (Teorema de Euclides)**.** *Existem infinitos números primos.*

Demonstração: Suponha, por contradição, que existe um número finito de números primos

$$p_1, p_2, \ldots, p_n.$$

Defina o número x como sendo o produto de todos eles mais 1, isto é,

$$x = p_1 p_2 \ldots p_n + 1.$$

Como $p_1 \geq 2$, temos $x \geq 3$. Logo, pela proposição 1.14, temos que x possui um divisor primo p. Logo podemos escrever $p = p_i$ para algum $i = 1, \ldots, n$. Seja $a = p_1 \ldots p_n$. Note que temos

$$a = p_i \left(p_1 p_2 \ldots p_{i-1} p_{i+1} \ldots p_n\right),$$

portanto $p_i \mid a$ e como $x = a + 1$ e temos que $p_i \mid a + 1$. Assim, $p_i \mid (a + 1) - a$, ou seja $p_i \mid 1$ e como consequência $p_i = 1$ o que contradiz o fato que $p_i > 1$. ■

O objetivo da subseção 1.9.1 é ver que qualquer número inteiro possui uma decomposição em fatores primos, que é uns dos teoremas importantes da teoria dos números, além de suas inúmeras aplicações. Este teorema é conhecido como o Teorema Fundamental da Aritmética.

Como dito acima, trata-se do fato de que todo número composto pode ser escrito como produto de fatores primos. Recordemos que na escola é usado um método para detectar os fatores primos de um número natural, que começa com a divisão do número pelo menor fator primo e o quociente dessa divisão pelo menor fator primo, e assim sucessivamente, cuja representação gráfica é a seguinte:

720	2
360	2
180	2
90	2
45	3
15	3
5	5
1	

Com isso podemos escrever a mesma fatoração obtida por meio da "árvore" de fatores quaisquer.

1.9.1 Teorema Fundamental da Aritmética

Comecemos com a demonstração de um lema que usaremos para a prova do teorema Fundamental da Aritmética.

Lema 1.9. *Sejam p e $q_1, \ldots, q_n$ números primos. Então $p \mid q_1 \cdots q_n$ se e somente se $p \in \{q_1, \ldots, q_n\}$.*

Demonstração: Se $p \in \{q_1, \ldots, q_n\}$ então é claro que temos $p \mid q_1 \cdots q_n$. Reciprocamente, se $p \mid q_1 \cdots q_n$ então, pelo lema 1.6 (veja seção 1.5, pg. 68), temos que $p \mid q_i$ para algum i. De que q_i é um número primo e que $p \neq 1$, concluímos que $p = q_i$. ■

Teorema 1.7 (Teorema Fundamental da Aritmética)**.** *Todo número inteiro a composto pode ser escrito de uma única forma como*

$$a = p_1 p_2 \ldots p_n,$$

sendo n um número natural (de fatores) e $p_1, p_2, \ldots, p_n$ números primos verificando $p_1 \leq \cdots \leq p_n$.

Observação 1.18. A exigência do teorema Fundamental da Aritmética de que os fatores apareçam ordenados em forma crescente é para garantir a unicidade da decomposição.
Note que no caso do número 720, pode ser escrito como

$$720 = 2^4 \cdot 3^2 \cdot 5,$$

onde temos ordenados os fatores em forma crescente e associando fatores iguais para formar as potências correspondentes a um mesmo fator.

Vamos a seguir fazer a prova do teorema 1.7.

Demonstração: (Teorema Fundamental da Aritmética] Note que basta provar o teorema para número naturais compostos, pois a fatorização em fatores primos de um número inteiro negativo é obtida achando a fatorização do seu valor absoluto e multiplicando-a por -1.
Logo, podemos pensar a como um número natural e usar o princípio de indução.

- $a = 2$ temos que $a = 2$ é a única fatoração de a.
- $a > 2$ suponha que o teorema é verdadeiro para todo número natural menor ou igual a a.

Pela proposição 1.13 temos a existência de inteiros $1 < b < a$ and $1 < c < a$ tal que $a = bc$. Se esse números são primos o teorema fica demonstrado. Suponha b composto. Então, pela hipótese indutiva, temos que b possui uma fatoração em fatores primos $p_1 \times \cdots \times p_m$ e portanto $a = c \times p_1 \times \cdots \times p_n$. Agora, se c for primo, temos finalizada a prova. Caso contrário usamos novamente a hipótese indutiva para c para decompor c em fatores primos $q_1 \times \cdots \times q_s$. Como resultado teremos

$$a = \overbrace{p_1 \times \cdots \times p_m}^{b} \times \overbrace{q_1 \times \cdots \times q_s}^{c},$$

que é a fatoração prima procurada de a.

Para provar a unicidade da fatoração em fatores primos, supomos que temos duas fatorações

$$p_1 \cdots p_m \;=\; q_1 \cdots q_n, \tag{1.33}$$

onde $q_1 \leq \cdots \leq q_n$ são fatores primos. Queremos provar que $m = n$ e que $p_i = q_i$ para todo i. Vamos supor então que $m \leq n$ e chegar a uma contradição. Procedemos por indução no número natural m.

$m = 1$ Temos que $p_1 = q_1 \cdots q_n$. Como p_1 é primo temos que a única forma da igualdade ser válida é que $n = 1$ e $p_1 = q_1$.

Se $m > 1$, segue do lema 1.9 que p_m é o maior divisor primo de $p_1 \cdots p_m$ e q_n é o maior divisor primo de $q_1 \cdots q_n$. Assim, como $p_1 \cdots p_m = q_1 \cdots q_n$, concluímos que $p_m = q_n$. Dividindo a expressão 1.33 por p_m obtemos

$$p_1 \cdots p_{m-1} \;=\; q_1 \cdots q_{n-1}.$$

Neste momento podemos usar a hipótese indutiva para concluir a unicidade. ■

Lembremos como fazíamos na escola para achar o máximo divisor comum de dois números usando a fatorização em fatores primos de um número inteiro.

Exemplo 1.24. Queremos saber o MDC de $a = 600$ e $b = 252$. Decompondo em fatores primos ambos os números, obtemos

$$\begin{aligned} 600 &= 2^3 \cdot 3^1 \cdot 5^2; \\ 252 &= 2^2 \cdot 3^2 \cdot 7. \end{aligned}$$

Assim, tomando os fatores comuns para garantir a existência de um divisor comum, o máximo desses divisores será

$$\mathrm{MDC}(600, 252) = 2^2 \cdot 3^1,$$

ou seja, o produto de fatores comuns elevados ao menor expoente.

Em geral a fatoração por primos não é uma tarefa fácil, por isso o algoritmo de Euclides é bem mais rápido na computação manual.

Outra consequência do teorema Fundamental da Aritmética é a possibilidade de achar o menor múltiplo comum a dois números inteiros positivos. Vejamos isto na próxima seção.

1.10 Mínimo múltiplo comum

Começemos com uma motivação. Para conseguir um bom rendimento de uma máquina, o engenheiro de uma fábrica recomenda que o óleo seja trocado a cada 600 horas de uso e o filtro que refrigera a máquina a cada 800 horas de uso. A questão é qual seria a quantidade mínima n de horas para conseguir trocar o óleo e o filtro ao mesmo tempo.

Deveríamos ter n múltiplo de 600 e 800 simultaneamente. Facilitando as contas, pensemos em $m = \frac{n}{100}$. Estamos procurando múltiplos comuns a 6 e 8 que vêm representados no seguintes conjuntos

$$M(6) = \{6,\ 12,\ 18,\ 24,\ 30, \ldots\} \text{ e } M(8) = \{8,\ 16,\ 24,\ 32,\ 40, \ldots\},$$

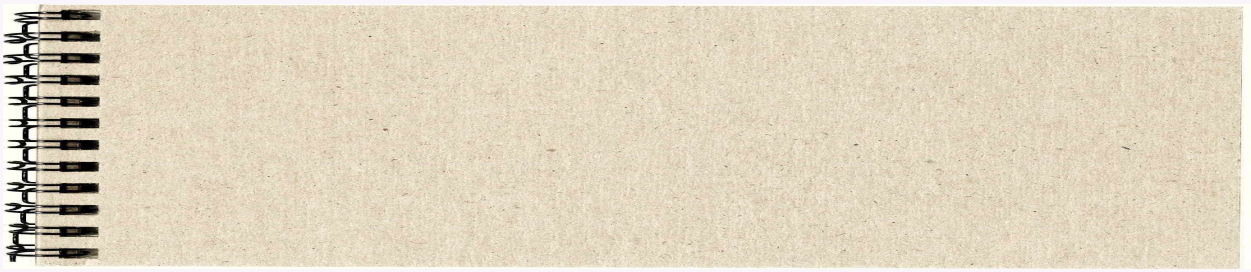
onde a notação $M(a)$ representa os múltiplos do número a. Notamos que o primeiro múltiplo comum na listas é o número 24, que seria a resposta a nossa questão para o valor de m. Logo a resposta é $n = 2.400$ horas.

Dizemos que 24 é o mínimo múltiplo comum aos números 6 e 8. Denotamos $\mathrm{MMC}(a, b)$ ao menor múltiplo comum dos números a e b.

Desafio!

Em um campeonato intedisciplinar no campus da UFU, a equipe de volei feminino da matemática tem uma partida a cada 48 horas e a equipe masculina a cada 56 horas. Suponha que ambas as equipes jogam a partida inaugural à mesma hora. Quantas horas depois jogam no mesmo horário?

Responda à questão usando os conjuntos de múltiplos de 48 e 56.



Clique aqui para ver a resposta.

Formalizando as ideias, dados a e b, o conjunto $M(a, b) = M(a) \cap M(b)$ dos múltiplos positivos em comum de a e b é não vazio, pois $a \cdot b \in M(a, b)$. Pelo axioma da boa ordenação, $M(a, b)$ possui um menor elemento m.

Chamamos esse número de Mínimo Múltiplo Comum de a e b e denotamos $m = \mathrm{MMC}(a, b)$.

Vamos caracterizar o $\mathrm{MMC}(a, b)$ pelo produto $a \cdot b$ e o $\mathrm{MDC}(a, b)$. Para isso precisamos do seguinte lema.

Lema 1.10. *Dados a e b números inteiros então se verifica que*

$$\min(a, b) + \max(a, b) = a + b.$$

Demonstração: Suponha que $a \geq b$. Caso contrário procedemos da mesma forma. Então,

$$\max(a, b) = a \quad \text{e} \quad \min(a, b) = b,$$

de onde, somando $a + b$, obtemos o resultado. ■

Proposição 1.15. *Sejam a e b dois inteiros positivos. Então,*

$$a \cdot b = \mathrm{MMC}(a, b) \cdot \mathrm{MDC}(a, b). \tag{1.34}$$

Demonstração: Vamos supor que

$$a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n} \quad \text{e} \quad b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}.$$

Da forma que calculamos o $\mathrm{MDC}(a, b)$, temos que

$$\mathrm{MDC}(a, b) = p_1^{\min(a_1, b_2)} p_2^{\min(a_2, b_2)} \ldots p_n^{\min(a_n, b_n)}$$

e também, da forma que calculamos o $\mathrm{MMC}(a, b)$ temos que

$$\mathrm{MMC}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \ldots p_m^{\max(a_n, b_n)}.$$

Assim, temos que

$$\begin{aligned}
\mathrm{MMC}(a, b) \cdot \mathrm{MDC}(a, b) &= p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \ldots p_n^{\max(a_n, b_n)} p_1^{\min(a_1, b_2)} p_2^{min(a_2, b_2)} \ldots p_n^{\min(a_n, b_n)} \\
&= p_1^{\max(a_1, b_1) + \min(a_1, b_1)} p_2^{\max(a_2, b_2) + \min(a_2, b_2)} \ldots p_m^{\max(a_n, b_n) + \min(a_n, b_n)} \\
&= p_1^{a_1 + b_1} p_2^{a_2 + b_2} \ldots p_n^{(a_n + b_n)} \\
&= p_1^{a_1} p_2^{a_2} \ldots p_m^{a_n} p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n} = ab,
\end{aligned}$$

como queríamos demonstrar. ■

A proposição 1.15 nos fornece uma maneira de calcular o mínimo comum múltiplo sem a necessidade de encontrar a fatoração prima dos números. Lembre que a forma tradicional, que

ensinamos na escola, de encontrar o mínimo comum múltiplo, é encontrando a fatoração prima de ambos os números e fazendo o produto dos fatores primos comuns e não comuns elevados ao maior expoente. Isto é útil para o caso de números pequenos, como 54 e 66, cujas decomposições são

$$\begin{array}{r|l} 66 & 2 \\ 33 & 3 \\ 11 & 11 \\ 1 & \end{array} \qquad \begin{array}{r|l} 54 & 2 \\ 27 & 3 \\ 9 & 3 \\ 3 & 3 \\ 1 & \end{array}$$

$$66 = 2 \cdot 3 \cdot 11 \qquad 54 = 2 \cdot 3^3$$

de onde $\text{MMC}(66, 54) = 2 \cdot 3^3 \cdot 11 = 594$.

Note que, usando a proposição 1.15, o cálculo seria feito achando o $\text{MDC}(66, 54)$, e que podemos calculá-lo usando o algoritmo de Euclides:

	1	4	2
66	**54**	12	6
12	6	**0**	

Assim, $\text{MMC}(66, 54) = \frac{66 \cdot 54}{\text{MDC}(66,54)} = 594$.

Já no caso de números muito grandes, a decomposição de números em fatores primos pode-se tornar muito longa. Veja o seguinte exemplo

Exemplo 1.25. Você teria coragem de fazer a fatoração prima de $2.345.444$ e 150.400 para achar o mínimo múltiplo comum desses números? Este é um verdadeiro desafio! Pois veja, com ajuda de uma calculadora, podemos achar $\text{MMC}(2.345.444, 150.400)$ usando a mesma técnica que fizemos com 66 e 54 no exemplo anterior.
Vamos achar o máximo divisor comum usando o algoritmo de Euclides:

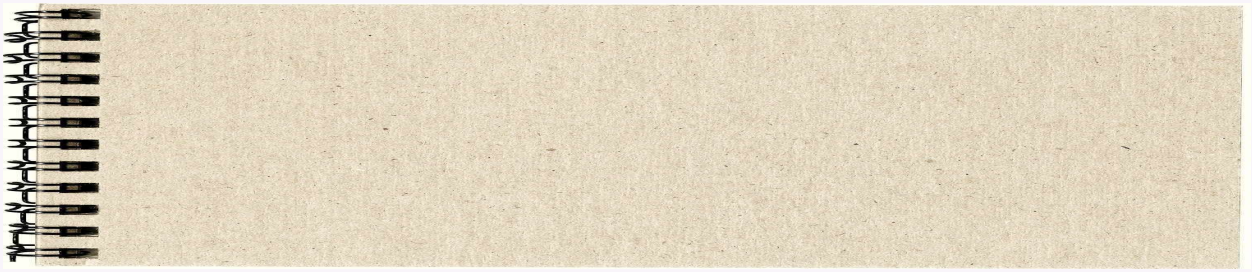
	15	1	1	2	7	6
2.345.444	**150.400**	89.444	60.956	28.488	3.980	628
89.444	60.956	28.488	3.980	628	214	

	2	1	25	2
628	212	204	8	**42**
204	8	4	**0**	

de onde $\text{MDC}(2.345.444, 150.400) = 4$. Assim $\text{MMC}(2.345.444, 150.400) = \frac{2.345.444 \cdot 150.400}{4} = 88.188.694.400$!

Desafio!

Calcule o $\mathrm{MMC}(545.327, 245.147)$ usando a proposição 1.15.



Clique aqui para ver a resposta.

Observação 1.19. No caso que $\mathrm{MDC}(a, b) = 1$ a igualdade da proposição 1.15 fica $\mathrm{MMC}(a, b) = a \cdot b$. Portanto o mínimo múltiplo comum de a e b é igual ao produto de a por b.

Por exemplo, do fato de que $\mathrm{MDC}(3, 8) = 1$, obtemos que o mínimo múltiplo comum de 3 e 8 é o produto $3 \cdot 8$. Vamos usar esta ferramenta no seguinte exemplo.

Exemplo 1.26. Vamos determinar todos os números naturais n tais que $\mathrm{MMC}(n, 130) = 260$. Por definição de mínimo múltiplo comum, $n \mid 260 = 2^2 \cdot 5 \cdot 13$ e $130 = 2 \cdot 5 \cdot 13$. Assim da fatoração de n em números primos só podem aparecer $2,\ 5$ e 13 elevados a potências

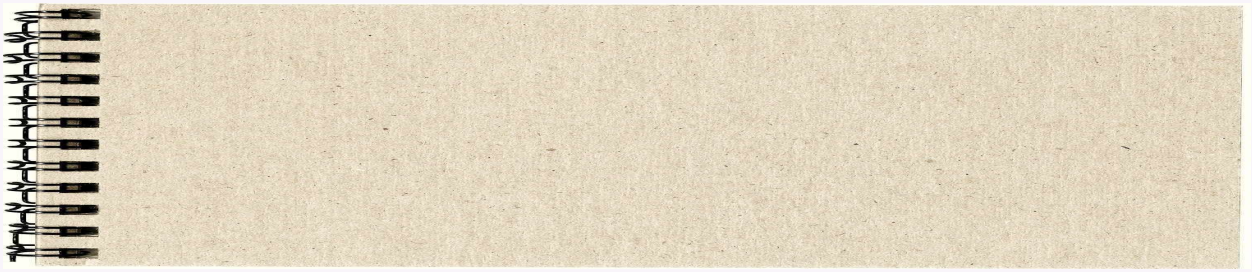
$$n = 2^2 \cdot 5^s \cdot 13^t \text{ com } 0 \leq s \leq 1,\ 0 \leq t \leq 1.$$

Analisamos todas as possibilidades:

1. se $s = t = 0$, então $n = 2^2 = 4$, que verifica $\mathrm{MMC}(n, 130) = 260$
2. $s = 0$ e $t = 1$, então $n = 2^2 \cdot 13 = 52$, que verifica $\mathrm{MMC}(n, 130) = 260$;
3. se $s = 1$ e $t = 0$, então $n = 2^2 \cdot 5 = 20$, que verifica $\mathrm{MMC}(n, 130) = 260$;
4. se $s = 1$ e e $t = 1$ então $n = 2^2 \cdot 5 \cdot 13 = 260$, que verifica $\mathrm{MMC}(n, 130) = 260$. Portanto, as soluções de nossa questão são $n = 4,\ 20,\ 52,\ 260$.

Desafio!

Encontrar todos os naturais a e b tais que $\mathrm{MMC}(a,b) = 1.500$ e $\mathrm{MDC}(a,b) = 10$.



Clique aqui para ver a resposta.

1.11 Respostas aos desafios do módulo 1

- Desafio da página 20.

  A sequência dos números ímpares como função de domínio natural pode ser escrita como

  $$f(n) = 2 \cdot n + 1 \quad \text{para todo número } n \text{ natural.}$$

  Também pode ser escrita como

  $$f(n) = 2 \cdot n - 3 \quad \text{para todo número } n \leq 2 \text{ natural,}$$

  onde aqui o domínio é o conjunto indutivo $\{n, \text{ natural }, n \geq 2\}$.

- Desafio da página 23.

  (Brasil,Brasília) e (Argentina, Buenos Aires) pertencem à relação. (Argentina, Brasília) e (Brasil, Buenos Aires) não pertencem à relação.

- Desafio da página 26

  Seja o conjunto $X = \{\{1,2\},\{1\},\ \{2\}\}$. Temos que para cada par de conjuntos formado a partir dos elementos de X obtemos um único conjunto que está em X. De fato, chamando de U à operação em X, temos

  $$\begin{array}{l} U(\{1\},\{1\}) = \{1\}; \\ U(\{2\},\{2\}) = \{2\}; \\ U(\{1\},\{2\}) = \{1,2\}; \\ U(\{2\},\{1\}) = \{2,1\} = \{1,2\}; \end{array}$$

- Desafio da página 29.

  $$\begin{array}{rcl} \sum_{i=2}^{i=4} \frac{i+1}{i-1} & = & \frac{2+1}{2-1} + \frac{3+1}{3-1} + \frac{4+1}{4-1} \\ & = & 3 + 2 + \frac{5}{3} = \frac{20}{3} \end{array}$$

$$15 + 18 + 21 + 24 + 27 = \sum_{i=5}^{i=9} 3i$$

$$\sum_{n=0}^{n=1} (n+1)n = 0(0+1) + 1(1+1) = 2$$

$$\tfrac{1}{2} + \tfrac{1}{4} + \tfrac{1}{8} + \tfrac{1}{16} = \sum_{i=1}^{i=4} \tfrac{1}{2^i}$$

$\sum_{n=1}^{135} n = \frac{135 \cdot 136}{2}$ seria a forma estendida. Sinteticamente escrevemos $\mathcal{P}(135)$.

- Desafio da página 33. A resposta é negativa pois $10/5 = 2$ e $5/10 = 0.4$. Assim a divisão de números não tem a propriedade comutativa. Um outro exemplo de operação que não é comutativa é a raiz $n-$ésima de um número positivo. Veja que $\sqrt[3]{2} \neq \sqrt[2]{3}$.

- Desafio da página 34.

  Temos que pela (1.8)

  $$\begin{aligned} a^2 &= a^1 \cdot a = a1 \cdot a; \\ a^3 &= a^2 \cdot a = a \cdot a \cdot a; \\ &\cdots \\ a^n &= \underbrace{a \cdot a \cdots a}_{n \text{ fatores}}. \end{aligned}$$

  Note que estamos usando a associativa do produto!

- Desafio da página 36.

  Vamos fixar m e demonstrar usando indução em n. Temos que

  $$(a \cdot b)^1 = a \cdot b = a^1 \cdot b^1,$$

  que comprova que $\mathcal{P}(1)$ é verdadeira.

  A seguir demonstramos o teorema indutivo:

  Hipotese: $\mathcal{P}(n)$ é verdadeira

  Tese: $\mathcal{P}(n+1)$ é verdadeira, que é equivalente a mostrar que $(a \cdot b)^{n+1} = a^{n+1} \cdot b^{n+1}$.
  Demonstrando o teorema indutivo:

  $$\begin{aligned} (a \cdot b)^{n+1} &= (a \cdot b) \cdot (a \cdot b)^n, && \text{por definição de potenciação} \\ &= (a \cdot b) \cdot (a^n \cdot b^n) && \text{usando a hipótese indutiva} \\ &= (a \cdot a^n) \cdot (b \cdot b^n) && \text{usando a comutativa e associativa da adição} \\ &= a^{n+1} \cdot b^{n+1} && \text{por definição de potenciação,} \end{aligned}$$

  de onde obtemos a tese indutiva.

- Desafio da página 37. Suponha que $n \geq m$ e $n \geq m$ simultaneamente. Queremos provar que $m = n$. Temos por hipótese que existem k e r números naturais tais que $n = m + k$

e $m = n + r$. Assim, temos que $n = (n + r) + k = n + (r + k)$. Pela lei de cancelamento (veja a propriedade 1.1, pg. 33), temos $r + k = 0$ de onde $r = 0$ e $k = 0$, o que mostra que $m = n$.

- Desafio da página 38.

> **Definição 1.29.** *Diz-se que* $m \in \mathbb{N}$ *é o* máximo *de um conjunto* $A \subset \mathbb{N}$ *se* $m \geq a$ *para todo* $a \in A$.

Um exemplo de máximo de um conjunto é tomando o mesmo conjunto do exemplo 1.11, $A = \{3, 10, 4, 100, 12\}$ e verificando que 100 é máximo de A. De fato temos $3 < 100$, $4 < 100$, $10 < 100$ e $12 < 100$ além que $100 \leq 100$. Assim checando que 100 é maior que TODOS os elementos de A, então por definição 1.29, 100 é o mínimo de A.

- Desafio da página 40 De acordo com a definição 1.8 (veja na página 24), temos que verificar três propriedades:

  1. Reflexiva: $(m, n)\ R\ (m, n)$ por definição de R;
  2. Simétrica: $(m, n)\ R\ (m_1, n_1)$ significa que $m - n = m_1 - n_1$ que a mesma coisa que $m_1 - n_1 = m - n$. , o que equivale a dizer, por definição de R, que $(m_1, n_1)\ R\ (m, n)$;
  3. Transitiva: se $(m, n) \sim (m_1, n_1)$ e $(m_1, n_1) \sim (m_2, n_2)$, então, por definição de R, temos
  $$\begin{array}{l} m - n = m_1 - n_1, \\ \text{o que implica } m - n = m_2 - n_2, \\ m_1 - n_1 = m_2 - n_2, \end{array}$$
  que por definição de R, significa que $(m, n)\ R\ (m_2, n_2)$

- Desafio da página 41

$$z_1 = [(130, 2)] = 128,\ z_2 = [(1, 8)] = -7,\ z_3 = [(1400, 1400)] = 0 \text{ e}$$
$$z_4 = [(60, 61)] = -1.$$

- Desafio da página 42.

De acordo com a definição 1.15 temos que

$$z_1 + z_2 = [(122, 55)] + [(202, 11)] = [(324, 66)],$$

e pela observação 1.6 temos como resultado o número natural $[(324, 66)] = 258$.

$$z_3 + z_4 = [(12, 45)] + [(1, 10)] = [(13, 55)] = -42,$$

- Desafio da página 51

$$D(14) = \{\pm 1, \pm 2, \pm 7, \pm 14\};$$
$$D(-6) = \{\pm 1, \pm 2, \pm 3, \pm 6\};$$
$$D(13) = \{\pm 1, \pm 13\};$$
$$D(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}.$$

Note que $D(6) = D(-6)$ e que todos os conjuntos contém ± 1.

- Desafio da página 56

$2 = 2 \cdot 6 + (-1) \cdot 10$. Como todo número par é da forma $2k$ então multiplicando por k a expressão da combinação linear de 2 obtemos

$$2k = (2k) \cdot 6 + (-k) \cdot 10,$$

o que mostra que todo número par é combinação linear de 6 e 10.

- Desafio da página 59

Primeiramente dividimos 1.678 por75

$$\begin{array}{r|l} 1678 & 75 \\ \cline{2-2} 28 & 22 \end{array}$$

obtendo

$$1.678 = 22 \cdot 75 + 28,$$

de onde $1.678 = (-1)22 \cdot (-1)75 + 28$ e a resposta é $q = -22$ e $r = 28$.

- Desafio da página 60

Para resolver a questão de dividir -345 entre -13, usamos o resultado de dividir 345 por 13, e escrevemos

$$\begin{aligned} -345 &= 26 \cdot (-13) - 7 \\ &= 26 \cdot (-13) - 7 + 13 - 13 \\ &= (26 + 1) \cdot (-13) + 13 - 7 \\ &= 27 \cdot (-13) + 6, \end{aligned}$$

portanto $q = 27$ e $r = 6$.

1. Dividindo 2.311 por 111 obtemos

$$\begin{array}{r|l} 2311 & 111 \\ \cline{2-2} 91 & 20 \end{array},$$

ou seja, $2.311 = 20 \cdot 111 + 91$. Multiplicando ambos os membros por -1, obtemos

$$\begin{aligned} -2.311 &= -(20 \cdot 111 + 91) \\ &= 20 \cdot (-111) - 91 \\ &= (20 + 1) \cdot (-111) + 111 - 91 \\ &= 21 \cdot (-111) + 20, \end{aligned}$$

portanto $q = 21$ e $r = 20$.

2. Dividindo 37 por 5, obtemos $37 = 7 \cdot 5 + 2$. Multiplicando ambos os membros por -1, obtemos

$$\begin{aligned} -37 &= 7 \cdot (-5) - 2 \\ &= 7 \cdot (-5) - 2 + 5 - 5 \\ &= (7 + 1) \cdot (-5) + 5 - 2 \\ &= 8 \cdot (-5) + 3, \end{aligned}$$

portanto $q = 8$ e $r = 3$.

- Desafio da página 63 Temos que

$$D(-18) = \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18\}.$$

$$D(30) = \{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30\}.$$

Portanto, o conjunto dos divisores comuns é o conjunto interseção

$$D(-18, 30) = \{\pm 1, \pm 2, \pm 3, \pm 6\}.$$

Assim, o maior divisor comum a -18 e 30 é 6.

Da mesma maneira podemos calcular o maior divisor comum de -12 e -36:

$$D(-12, -36) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}.$$

Portanto,. o maior divisor comum a -12 e -36 é 12.

Note que o maior divisor comum sempre é positivo!

- Desafio da página 70.

Calculamos primeiramente $\mathrm{MDC}(456, 203)$. Efetuando a sucessivas divisões, obtemos a seguinte tabela:

	2	4	16	1	2
456	**203**	50	3	2	1
50	3	2	1	**0**	

$=\mathrm{MDC}(456, 203) = 1$

Agora vamos calcular $\mathrm{MDC}(5.560, 3.535)$, obtemos

	1	1	1	2	1	13	1	2	2
5.560	**3.535**	2025	1510	515	480	35	25	10	5
2025	1510	515	480	35	25	10	5	**0**	

$=\mathrm{MDC}(5.560, 3.535) = 5$

- Desafio da página 72.

	2	1	5	2
37	**13**	11	2	1
11	2	1	**0**	

Assim, os números $11,\ 2$, e 1 podem ser escritos como a seguir:

$$\begin{aligned} 11 &= 37 - 2 \cdot 13 \\ 2 &= 13 - 11 \cdot 1 \\ 1 &= 11 - 5 \cdot 2 \end{aligned}$$

Substitutindo essas equações, podemos expressar o máximo divisor comum como combinação linear dos números 37 e 13 como segue

$$\begin{aligned} 1 &= 11 - 5 \cdot \overbrace{(13 - 11)}^{2} \\ &= (-5) \cdot 13 + 6 \cdot 11 \\ &= (-5) \cdot 13 + 6 \cdot \overbrace{(37 - 2 \cdot 13)}^{11} \\ &= 6 \cdot 37 - 17 \cdot 13. \end{aligned}$$

Assim, os coeficientes de Bézout são 6 e -17.

- Desafio da página 75.

Seja o conjunto $A = \{1.009,\ 1.013,\ 1.021,\ 1.031,\ 1.033,\ 1.039,\ 1.049,\ 1.051$. Vamos demonstrar que são números primos.

Tomemos o maior dos números e encontremos com a calculadora uma aproximação por defeito da raiz quadrada de 1051 que seja primo. Vemos que esse número é 31. De novo com calculadora em mão, pode-se ver que não há nenhum divisor dos compreendidos entre 2 e 31. Note que basta procurar divisores primos: $2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29$ e 31.

- Desafio da página 81. Para conhecer a resposta, basta achar o mínimo comum múltiplo entre 48 e 56. Usando o conjunto de múltiplos, temos que

$$M(48) = \{48,\ 96,\ 144,\ 192,\ 240,\ 288,\ 336,\ 384, \ldots\};$$

$$M(56) = \{56,\ 112,\ 168,\ 224,\ 280,\ 336,\ 392, \ldots\}$$

observando que o menor múltiplo em comum é 336. Assim depois de 336 horas da inauguração do campeonato, as equipes femenina e masculina irão jogar simultaneamente.

- Desafio da página 84.

Calculamos primeiramente $\mathrm{MDC}(545.327, 245.147)$ usando o algoritmo de Euclides:

	2	4	2	5	
545.327	**245.147**	55.033	25.015	5.003	5.003=
55.033	25.015	5.003	**0**		

Assim, $5.003 = \mathrm{MDC}(545.327, 245.147)$, e usando a proposição 1.15, obtemos que

$$\mathrm{MMC}(545.327, 245.147) = \frac{545.327 \cdot 245.147}{5003} = 26.721.023$$

- Desafio da página 85.

  Vamos encontrar todos os naturais a e b tais que $\mathrm{MMC}(a, b) = 1.500$ e $\mathrm{MDC}(a, b) = 10$.

  Sabemos que se a e b são os números que queremos achar, então

  $$a \cdot b = \mathrm{MDC}(a, b) \cdot \mathrm{MMC}(a, b) = 10 \cdot 1.500 = 15.000.$$

  Veja que $15.000 = 2^3 \cdot 3 \cdot 5^3$, fatoração do produto $a \cdot b$. Logo, as possíveis fatorações de a e b são

  $$a = 2^r \cdot 3^s \cdot 5^t \text{ e } b = 2^{3-r} \cdot 3^{1-s} \cdot 5^{4-t},$$

  onde, levando em conta que $\mathrm{MDC}(a, b) = 10$, os fatores primos 2 e 5 aparecem na decomposição de 10 elevados a expoente 1. Assim, se fosse $t = 2$ teriamos um MDC com um fator primo 5 elevado ao quadrado, que não é possível. Assim, devemos ter

  $$0 \leq r \leq 2,\ 0 \leq s \leq 1,\ 0 \leq t \leq 3 \text{ e } t \neq 2.$$

  Fazendo os cálculos, obtemos os pares soluções (a, b):

  $$(10, 1.500),\ (20, 750),\ (30, 500),\ (60, 250).$$

No término do módulo II, o aluno estará familiarizado como os seguintes conceitos:

- ▷ Congruência.
- ▷ Aritmética dos restos.
- ▷ Congruência e divisibilidade.
- ▷ Congruências lineares e equações diofantinas lineares.

2.1 Congruência

Parece que tudo começou muito tempo atrás quando alguém notou que, por exemplo, se somarmos $25 + 13$, o resto da divisão inteira de 25 por 11

$$\begin{array}{r|l} 25 & 11 \\ \hline 3 & 2 \end{array}$$

que é 3 se soma ao resto da divisão inteira de 13 por 11,

$$\begin{array}{r|l} 13 & 11 \\ \hline 2 & 1 \end{array}$$

que é 2, para dar exatamente o resto da divisão inteira de 38 por 11

$$\begin{array}{r|l} 38 & 11 \\ \hline 5 & 3 \end{array}$$

que é $5 = 2 + 3$! Não foi só isso, na multiplicação também notaram essa propriedade: o resto da divisão inteira de 23×14 por 11

$$\begin{array}{r|l} 325 & 11 \\ \hline 6 & 29 \end{array}$$

que é exatamente $6 = 2 \times 3$.

Os primeiros a observar essas curiosidades foram os gregos, chineses e indianos, que gostavam de resolver problemas envolvendo divisões inteiras e seus restos. A teoria porém não evoluiu muito até que Gauss fez sua maior contribuição à teoria dos números com o seu livro *Disquisitiones Arithmeticae*, (traduzido como Investigações na Aritmética) publicado em 1801. Gauss introduz principalmente a notação de congruência para a relação entre os números inteiros e seus restos da divisão por um mesmo número inteiro.

Por exemplo, qual é a relação entre os números inteiros 4, 11 e 18 quando divididos por 7?

$$\begin{array}{r|l} 4 & 7 \\ \hline 4 & 0 \end{array} \qquad \begin{array}{r|l} 11 & 7 \\ \hline 4 & 1 \end{array} \qquad \begin{array}{r|l} 18 & 7 \\ \hline 4 & 2 \end{array}$$

O número 7 no exemplo é chamado de módulo e o estudo das aritmética produzida pela relação entre os números inteiros pelo módulo é conhecido como **aritmética modular**.

Começamos o estudo teórico com a definição de congruência.

Definição 2.1. *Sejam $m \geq 0$, a e b números inteiros. Diz-se que a é congruente com b no módulo m se e somente se*

$$m \mid a - b.$$

Denotamos o conceito definido em 2.1 por $a \equiv b \pmod{m}$. A notação $a \not\equiv b \pmod{m}$ é a negação de $a \equiv b \pmod{m}$.

Exemplo 2.1.

1. $25 \equiv 1 \pmod{4}$ porque $4 \mid 24$;
2. $a \equiv b \pmod{1}$ para todo a, b porque 1 divide qualquer número;

Desafio!

Agora você explica, no caderno, o porquê das afirmações $1 \equiv -3 \pmod{4}$ e $25 \not\equiv 2 \pmod{4}$.

Clique aqui para ver a resposta.

Note também que

1. $a \equiv b \pmod{0}$ se e somente se $a = b$ para todo $a,\ b$, isto porque 0 somente divide 0.

Lembre das reflexões que fizemos sobre o assunto de DIVISOR de 0 no módulo I. Não deixe de ler novamente essas reflexões!

2. quando dois números inteiros são ambos pares ou ambos ímpares, então são congruentes no módulo 2.

O teorema a seguir justifica porque a teoria da congruência é conhecida como a aritmética dos restos, que foi, como apontado na introdução deste módulo, a forma em que historicamente esta teoria começou.

Teorema 2.1. *Para $m > 0$ e para todo a, b as expressões abaixo são equivalentes*

- $a \equiv b \pmod{m}$;
- *O resto da divisão inteira de a por m é o mesmo que o da divisão inteira de b por m.*

Demonstração: Suponha que $a \equiv b \pmod{m}$, r_1 o resto da divisão inteira a por m e r_2 o resto da divisão inteira b por m. Queremos provar que $r_1 = r_2$. Pela definição 2.1 temos que

$$m \mid a - b, \tag{2.1}$$

e pela definição de resto da divisão inteira de a por m e b por m temos que

$$a = mq_1 + r_1,\ 0 \leq r_1 < m \tag{2.2}$$

e

$$b = mq_2 + r_2,\ 0 \leq r_2 < m. \tag{2.3}$$

De (2.1) obtém-se

$$a - b = mt,$$

para algum t. Segue-se que

$$a = mt + b.$$

Usando (2.2) e (2.3), temos que

$$a = mq_1 + r_1 = m\,(q_2 + t) + r_2.$$

Como temos $0 \leq r_1 < m$ e $0 \leq r_2 < m$, pela unicidade do resto da divisão inteira, obtemos $r_1 = r_2$, como queriamos provar.

Reciprocamente, suponha que o resto da divisão inteira a por m é o mesmo da divisão inteira b por m. Seja $0 \leq r < m$ este resto. Então, por definição de divisão inteira, temos que

$$\begin{aligned} a &= mq_1 + r \\ \text{e} \\ a &= mq_2 + r \\ \text{e subtraindo membro a membro} \quad & \\ \hline a - b &= m\,(q_1 - q_2) \end{aligned}$$

Isto mostra que $m \mid a - b$ e pela definição 2.1 chegamos a que $a \equiv b \pmod{m}$. ■

Responda a esta questão: que dia da semana vai ser após sete dias depois de uma segunda–feira? Fácil de responder, correto? Você vai dizer: “obviamente” que vai ser outra segunda feira, uma vez que a semana tem 7 dias.

Outra pergunta interessante: e qual será o dia da semana depois de oito dias passados desde a segunda–feira? Já sei, você esta pensando que essa pergunta tem também uma resposta óbvia, que ... deve ser terça–feira.

Bom, já que você está achando fáceis todas as repostas, você vai responder rapidamente à pergunta: *qual será o dia da semana após* 16 *dias desde segunda–feira*. Desta vez vamos escrever um pouco, já que sabemos que

$$16 = 2 \times 7 + 2,$$

em outras palavras, passaram duas semanas e dois dias, logo, ainda é fácil afirmar que o dia 16 dias após uma segunda–feira deve ser uma quarta–feira.

O que estamos fazendo em cada um desses casos é encontrar o número de dias a partir de segunda–feira no módulo 7.
Em outras palavras, tudo o que você realmente precisa saber é um número entre 0 e 6, que lhe diz quantos dias a partir de segunda–feira você precisa contar para a frente, onde 0 é segunda–feira, 1 vai ser uma terça–feira, 2 significa que estaremos na quarta-feira, e assim por diante, até chegar a seis dias de segunda–feira, o que será um domingo.

Agora vamos para uma pergunta mais ousada... e ... que dia da semana será daqui a 5780 dias... sim!, supondo que hoje é segunda–feira.

Primeiramente vamos calcular a que valor entre 0 e 6 o número 5780 é congruente em módulo 7. Ou seja, basta calcular o resto da divisão inteira de 5780 por 7, para obter

$$\begin{array}{r|l} 5780 & 7 \\ \cline{2-2} 5 & 825 \end{array}$$

Assim, o dia da semana 5780 dias depois desta segunda–feira vai ser o dia da semana que vem 5 dias após a qualquer segunda feira ... que é sábado!

Para mais aplicações, recomendamos a leitura complementar

ARITMÉTICA MODULAR E ALGUMAS DE SUAS APLICAÇÕES

do Professor Ilydio Pereira de Sá - UERJ - Rio de Janeiro

Observação 2.1. Para entender a próxima subseção, estude primeiramente o que é uma relação de equivalência definida em um conjunto na seção 1.2.1.

2.1.1 A Congruência como Relação de Equivalência

A seguir vamos mostrar que a relação R definida por $a \equiv b \pmod{m}$ é uma *relação de equivalência* no conjunto $\mathbb{Z}$.

Teorema 2.2 (A Congruência é uma relação de equivalência)**.** *Para todo* $a,\ b,\ c$ *e* $m > 0$ *temos*

1. *Para todo* $a \in \mathbb{Z}$ *temos que* $a \equiv a \pmod{m}$ ***propriedade reflexiva****;*
2. *se* $a \equiv b \pmod{m}$ *então* $b \equiv a \pmod{m}$ ***propriedade simétrica****;*
3. *se* $a \equiv b \pmod{m}$ *e* $b \equiv c \pmod{m}$ *implica que* $a \equiv c \pmod{m}$ ***propriedade transitiva****.*

Demonstração:

Item 1. Como temos $a - a = 0 = 0 \cdot m$ então $m \mid a - a$ o que significa pela definição 2.1 que $a \equiv a \pmod{m}$.

Item 2. De que $a \equiv b \pmod{m}$, pela definição 2.1 temos que $m \mid a - b$.

Assim, $a - b = mq$ para algum número inteiro q. Multiplicando por -1 esta igualdade, obtemos $b - a = m(-q)$, que significa que $m \mid b - a$. Portanto, $b \equiv a \pmod{m}$.

Item 3. De que $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$ obtemos $m \mid a - b$ e $m \mid b - c$, pela definição 2.1. Pela propriedade de linearidade da divisão, obtemos qu $m \mid (a - b) + (b - c)$ ou em forma equivalente, $m \mid a - c$. Assim, concluímos que $a \equiv c \pmod{m}$. ■

Exemplo 2.2.

- Temos que $14 \equiv 8 \pmod{6}$, pois 6 divide $14 - 8 = 6$. Assim, como consequência da propriedade simétrica, temos que $8 \equiv 14 \pmod{6}$.
- Como $22 \equiv 10 \pmod{6}$ e $10 \equiv 4 \pmod{6}$, então, pela propriedade transitiva, temos que $22 \equiv 4 \pmod{6}$.

Notação 2.1. *Vamos denotar uma expressão do tipo*

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,\ n \geq 0$$

como um polinômio com coeficientes $a_n, \ldots, a_0$ *são números inteiros e* x *também assume valores inteiros.*

Teorema 2.3. *Sejam* $a \equiv b \pmod{m}$ *e* $c \equiv d \pmod{m}$*, então temos as seguintes afirmações:*

1. $a \pm c \equiv b \pm d \pmod{m}$;
2. $ac \equiv bd \pmod{m}$;
3. *se* $a \equiv b \pmod{m}$ *então* $ac \equiv bc \pmod{mc}$*, para todo* $c > 0$.
4. $a^n \equiv b^n \pmod{m}$ *para todo* $n \geq 1$;
5. $p(a) \equiv p(b) \pmod{m}$ *para todo polinômio* $p(x)$ *como descrito na notação 2.1.*

Demonstração:

1. Como temos que $a - c = a + (-c)$, basta provar a afirmação para a soma. Temos que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então, pela definição 2.1, $m \mid a - b$ e $m \mid c - d$.

   Pela linearidade da divisibilidade temos também que $m \mid (a - b) + (c - d)$

   ou seja $m \mid (a + c) - (b + d)$, concluindo que

   $$a + c \equiv b + d \pmod{m}.$$

2. Novamente usamos a definição 2.1 para afirmar que $m \mid a - b$ e $m \mid c - d$ e por linearidade obtém-se que

   $$m \mid c(a - b) + b(c - d).$$

   Note que $c(a - b) + b(c - d) = ca - bd$ de onde concluimos que

   $$m \mid ca - bd,$$

   o que prova que $ca \equiv bd \pmod{m}$ usando a definição 2.1 novamente.

3. Como $a \equiv b \pmod{m}$, então temos que $m \mid (a - b)$. Logo, existe um número inteiro k tal que $a - b = mk$ e, como resultado,

   $$ac - bc = mc(k).$$

   Isto mostra que $mc \mid (ac - bc)$ e, portanto, $ac \equiv bc \pmod{mc}$.

4. Podemos provar $a^n \equiv b^n \pmod{m}$ por indução em n. Deixamos isto como exercício para o leitor.

5. Provamos por indução no grau n do polinômio. Queremos provar que se $a \equiv b \pmod{m}$ então

$$c_n a^n + \cdots + c_0 \equiv c_n b^n + \cdots + c_0 \pmod{m}.$$

No caso de $n = 0$, temos que $c_0 \equiv c_0 \pmod{m}$.

Vamos supor que a proposição é verdadeira para $n = k$ isto é

$$c_k a^k + \cdots + c_1 a + c_0 \equiv c_k b^k + \cdots + c_1 b + c_0 \pmod{m}. \tag{2.4}$$

Pelo item 4 acima, temos que

$$a^{k+1} \equiv b^{k+1} \pmod{m}.$$

Como também é verdadeiro que $c_{k+1} \equiv c_{k+1} \pmod{m}$, usando o item 2 acima, obtemos que

$$c_{k+1} a^{k+1} \equiv c_{k+1} b^{k+1} \pmod{m}. \tag{2.5}$$

Aplicando o item 1 acima a (2.4) e (2.5), concluimos que

$$c_{k+1} a^{k+1} + c_k a^k + \cdots + c_0 \equiv c_{k+1} b^{k+1} + c_k b^k + \cdots + c_0 \pmod{m},$$

o que prova a propriedade para $k + 1$.

Isto completa a demonstração por indução e a deste item. ■

Exemplo 2.3.

- Temos que $50 \equiv 20 \pmod{15}$. Do item 1 do teorema 2.3 (veja pag. 98), temos que $50 + 5 = 55 \equiv 20 + 5 = 25 \pmod{15}$.

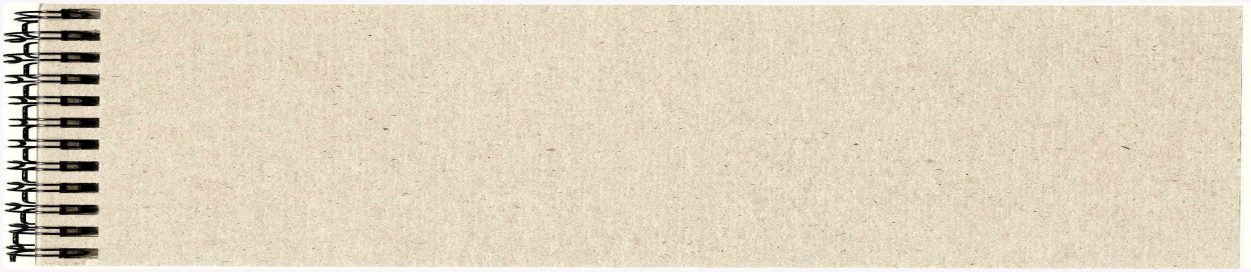
  Pela mesma propriedade, obtemos que$50 - 5 = 45 \equiv 20 - 5 = 15 \pmod{15}$.

- Temos que $19 \equiv 16 \pmod{3}$ e pela propriedade 2 do teorema 2.3, temos que $2(19) = 38 \equiv 2(16) = 32 \pmod{3}$.

- De que $19 \equiv 16 \pmod{3}$ pelo item 3 do teorema 2.3, temos que $2(19) \equiv 2(16) \pmod{2(3)}$, ou seja, $38 \equiv 32 \pmod{6}$.

Desafio!

Sejam $a,\ b$ e c números inteiros positivos tais que $a \equiv -1 \pmod 7$ e os restos da divisão inteira por 7 de b e c são 6 e 3, respectivamente. Encontre o resto da divisão inteira de $a+b+c$ por 7.

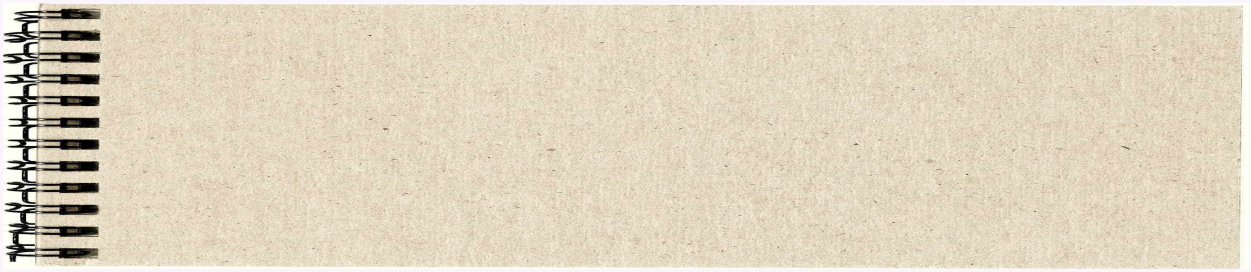


Clique aqui para ver a resposta.

Mais um desafio para calcular o resto de uma divisão inteira.

Desafio!

Calcule o resto da divisão inteira de 7^{25} por 3. Sem calculadora!



Clique aqui para ver a resposta.

Vamos calcular agora o dígito das unidades na representação decimal de 83^{1047} sem calcular o número! Só iremos usar a calculadora para encontrar as primeiras cinco potências de 83 e anotar os dígitos das unidades:

$$\begin{aligned} 83^0 &= 1 \\ 83^1 &= 83 \\ 83^2 &= 6.889 \\ 83^3 &= 571.787 \\ 83^4 &= 47.458.321 \end{aligned} \tag{2.6}$$

Note que os dígitos das unidades são $1,\ 3,\ 9,\ 7,\ 1, \ldots$, repetindo o primeiro dígito obtido no primeiro cálculo.

Será que irá se repetir essa sequência de dígitos para “sempre”?

Calculemos mais uma potência só para conferir a observação feita:

$$83^5 = 3.939.040.643.$$

... que é o mesmo valor seguinte de 1 na sequência de dígitos das unidades!
Como poderíamos provar isso?

Sabemos que temos uma representação decimal para 83^{1047} dada por $d_n \dots d_1 d_0$, com $d_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ de forma que

$$83^{1047} = d_n \cdot 10^n + \ldots + d_1 \cdot 10 + d_0,$$

ou, equivalentemente,

$$83^{1047} = 10(d_n \cdot 10^{n-1} + \ldots + d_1) + d_0,$$

o que implica que o resto da divisão inteira de 83^{1044} por 10 é d_0, já que $d_0 < 10$. Então “bastaria” encontrar esse resto da divisão por 10 para achar o dígito das unidades do número 83^{1047}. Significa que deveríamos procurar um número d_0 entre 0 e 9 tal que

$$83^{1047} \equiv d_0 \pmod{10}.$$

Agora iremos usar com força as propriedades do teorema 2.3. Pelos cálculos com a calculadora feitos em (2.6), temos que

$$83^4 = 47.458.321 \equiv 1 \pmod{10},$$

e pelo item 4 do teorema 2.3, elevando ambos os membros da $\equiv$ ao número k, obtém-se

$$(83^4)^k \equiv 1^k \pmod{10}. \tag{2.7}$$

Escrevendo o número $1047 = 4 \cdot 261 + 3$ e usando propriedades das potências de números naturais, chegamos a que

$$83^{1047} = 83^{4 \cdot 261 + 3} = 83^{4 \cdot 261} \cdot 83^3,$$

e usando os cálculos de (2.7) e que $83^3 \equiv 7 \pmod{10}$, concluímos pelo item 2 do teorema 2.3, que

$$83^{1047} \equiv 7 \pmod{10}.$$

Assim a resposta à pergunta do dígito das unidades é $d_0 = 7$.

Qual será a resposta à pergunta da repetição da sequência de digitos das unidades quando continuamos a elevar 83 a potências naturais?

Note que, aplicando as mesmas propiedades, podemos determinar o dígito das unidades de 83^n para qualquer n natural! Vamos conferir?

Efetuamos a divisão inteira de n por 4 para encontrar q e $0 \leq r \leq 3$, quociente e resto desta divisão. Assim,

$$83^n = 83^{4q+r} = 83^{4q} \cdot 83^r \equiv 83^r \pmod{10}.$$

Dos primeiros cáculos feitos em (2.6), os dígitos das unidades possíveis são $1,\ 3,\ 9$ e 7, correspondendo aos respectivos restos $r = 0,\ 1,\ 2,\ 3$.

Vamos praticar esta técnica?

Exemplo 2.4. Vamos encontrar o resto da divisão inteira de um número por outro escrito como expoente grande como, por exemplo, achar o resto da divisão inteira de $17^{15.689.876}$ por 3.

Vamos observar primeiramente que, sendo $17 \equiv 2 \pmod{3}$, então temos

$$17^k \equiv 2^k \pmod{3}. \tag{2.8}$$

Agora observe que efetuando a divisão inteira de $a = 2^k$ por 3, temos ± 1 como resto desta divisão inteira. De fato,

$$\begin{aligned} 2^0 &= 1 \equiv 1 \pmod{3} \\ 2^1 &= 2 \equiv -1 \pmod{3} \\ 2^2 &= 4 \equiv 1 \pmod{3} \\ 2^3 &= 8 \equiv -1 \pmod{3} \end{aligned}$$

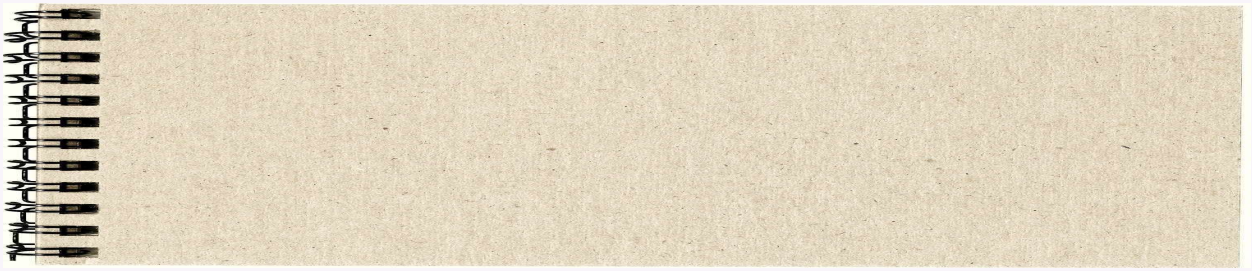
Também note que quando k é par o resto da divisão é 1. Desta afirmação e de (2.8),concluímos que a resposta à pergunta formulada é: o resto da divisão inteira de $17^{15.689.876}$ por 3 é 1.

Note que, na realidade, mostramos mais do que isso: para qualquer expoente diferente de 1, o resto da divisão inteira de 17^k por 3 é ± 1.

Para praticar ainda mais, aceite o seguinte desafio!

Desafio!

Ache o resto de divisão inteira de $23^{71.355}$ por 4.



Clique aqui para ver a resposta.

Uma aplicação teórica do teorema 2.3, relacionada com o último teorema de Fermat, é a proposição a seguir.

Proposição 2.1. *Seja a, b e c números inteiros tais que $a^2 + b^2 = c^2$. Então $3 \mid a$ ou $3 \mid b$.*

Demonstração: Suponha que 3 não divide a e 3 não divide b, ou seja, negamos o que queremos provar. Então, o resto da divisão inteira de a por 3 tem que ser 1 ou 2 e a mesma conclusão para a divisão inteira de b por 3. De que $1^2 \equiv 1 \pmod 3$ e $2^2 \equiv 1 \pmod 3$ obtemos pelo item 4 do teorema 2.3 que $a^2 \equiv 1 \pmod 3$ e $b^2 \equiv 1 \pmod 3$. Assim, pelo item 1 do teorema 2.3, concluímos que $c^2 \equiv 2 \pmod 3$. Ora, para c temos três possibilidades no módulo 3:

1. $c \equiv 0 \pmod 3$ e daí $c^2 \equiv 0 \pmod 3$;
2. $c \equiv 1 \pmod 3$ e daí $c^2 \equiv 1 \pmod 3$ ou $c \equiv 2 \pmod 3$
3. $c^2 \equiv 1 \pmod 3$, da mesma forma que demonstramos para a e b.

Logo, não podemos ter $c^2 \equiv 2 \pmod 3$. O que é verdadeiro é que $3 \mid a$ ou $3 \mid b$, como queríamos demonstrar. ■

2.2 Aritmética dos restos

O teorema 2.2 mostra que com a relação de equivalência congruência definida em $\mathbb{Z}$ temos, como resultado, um conjunto quociente (veja no módulo I a definição de conjunto quociente), $\mathbb{Z}/\equiv$, constituído por todas as classes de equivalências determinadas pela relação $\equiv$.

Vamos mostrar a seguir as classes de equivalências definidas em $\mathbb{Z}$ pela congruência módulo 2.

Dado o número inteiro a, temos dois diferentes restos da divisão inteira de a por 2:

1. $a = 2k + r_0$ com $r_0 = 0$;

2. $a = 2k + r_1$ com $r_1 = 1$.

Assim, a relação de congruência módulo 2 determina duas classes de equivalências, que estão definidas da seguinte maneira:

$$[0] = \{a \in \mathbb{Z},\ a \equiv 2 \pmod 0\} = \{a \in \mathbb{Z},\ a = 2k\}$$

$$[1] = \{a \in \mathbb{Z},\ a \equiv 2 \pmod 1\} = \{a \in \mathbb{Z},\ a = 2k + 1\}.$$

O conjunto quociente determinado pela relação de congruência módulo 2, é denotado por $\mathbb{Z}/2\mathbb{Z}$. Portanto, temos que

$$\mathbb{Z}/2\mathbb{Z} = \{[0], [1]\}.$$

Da mesma forma que para a congruência de módulo 2, podemos determinar as classes de equivalência orginidas pela relação de congruência módulo 3. Estas são três que denotaremos por $[0]$, $[1]$ e $[2]$, e definidas como:

$$\begin{aligned}[0] &= \{a \in \mathbb{Z},\ a = 3k\}\\ [1] &= \{a \in \mathbb{Z},\ a = 3k + 1\}\\ [2] &= \{a \in \mathbb{Z},\ a = 3k + 2\}\end{aligned}$$

O conjunto das classes é dado por

$$\mathbb{Z}/3\mathbb{Z} = \{[0], [1], [2]\}.$$

Note que em ambos os casos analisados as classes vêm determinadas pelos restos das divisões de um inteiro com o módulo de congruência. Vamos estudar como operar essas classes. Esta aritmética é conhecida como **aritmética dos restos**.

Definição 2.2. *Para* $[a],\ [b] \in \mathbb{Z}/\equiv$ *definimos*

$$[a] + [b] = [a + b];$$

$$[a][b] = [ab].$$

Exemplo 2.5. Para $m = 5$ temos que

$$[2] + [3] = [5], \text{ e}$$

$$[2][3] = [6].$$

Note que, como temos $5 \equiv 0 \pmod 5$ e $6 \equiv 1 \pmod 5$ obtemos $[5] = [0]$ e também que $[6] = [1]$. Portanto, podemos escrever

$$[2] + [3] = [0]$$

$$[2][3] = [1].$$

Um fato ao qual devemos prestar muita atenção é ao representante escolhido, já que podemos tomar qualquer número para identificar a classe. Note que, para $m = 5$, temos que

$$[7] = [2] \text{ e } [11] = [21]$$

logo *devemos* ter que

$$[7] + [11] = [2] + [21] \text{ e}$$

$$[7][11] = [2][21].$$

É isso verdade? Vejamos a seguir.

$$[7] + [11] = [18] \text{ e } [2] + [21] = [23].$$

Por outro lado, temos que $23 \equiv 18 \pmod 5$, porque $5 \mid 23 - 18$. Assim chegamos a que $[18] = [23]$, como queríamos demonstrar.

Também temos que $[7][11] = [77]$ e que $[2][21] = [42]$, de onde concluímos que $77 - 42 = 35$, e daí $5 \mid 35$. Isto mostra que $77 \equiv 42 \pmod 5$ ou, equivalentemente, que $[77] = [42]$. Ou seja, neste caso particular, a escolha dos representantes não muda o resultado da operação das classes. Vamos enunciar este fato em forma geral no próximo teorema.

Teorema 2.4. *Para qualquer $m > 0$ é verdadeiro que se $[a] = [b]$ e $[c] = [d]$, então*

$$[a] + [c] = [b] + [d] \qquad \textit{e} \qquad [a][c] = [b][d].$$

Demonstração: Esta afirmação é uma consequência imediata do teorema 2.3 (pag. 98). ■

Quando efetuamos a adição ou multiplicação em $\mathbb{Z}/m\mathbb{Z}$ para um inteiro positivo m, usando a definição 2.2 e devido ao teorema 2.4 podemos substituir o representante de uma classe $[a]$ por outro representante mais "conveniente", no sentido de facilitar as operações. Vejamos um exemplo deste comentário.

Exemplo 2.6. *Seja* $m = 151$. *Note que* $150 \equiv -1 \pmod{151}$ *e* $149 \equiv -2 \pmod{151}$, *portanto*

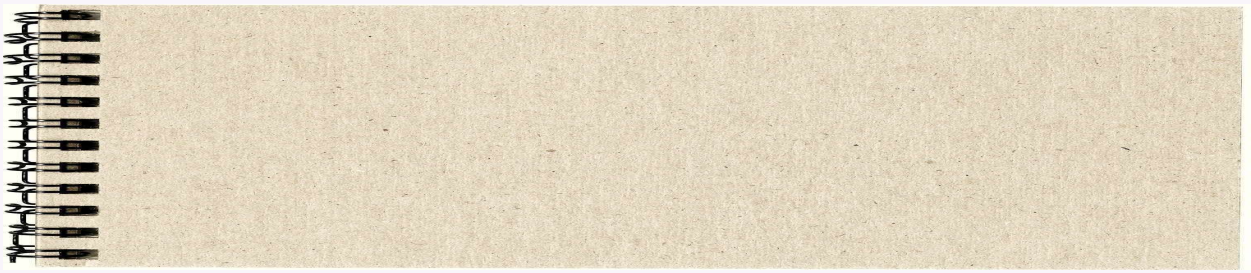
$$[150][149] = [-1][-2] = [2] \text{ e}$$

$$[150] + [149] = [-1] + [-2] = [-3] = [148],$$

onde esta última conclusão vem do fato de que $148 \equiv -3 \pmod{151}$.

Desafio!

Calcule $[89] + [55]$ e $[89] \cdot [55]$ em $\mathbb{Z}/44\mathbb{Z}$ usando outros representantes da classe.



Clique aqui para ver a resposta.

Note que, no desafio, usamos os restos da divisão inteira de 89 e 55 por 44 como representantes para fazer as operações. De forma de escolher o melhor representante da classe para efetuar as operações nos conjuntos $\mathbb{Z}/m\mathbb{Z}$, usaremos precisamente o teorema 2.1 (pag. 98) e de que, se temos $0 \leq r < m$, então $r \equiv r \pmod{m}$. Isto fica claro porque temos

$$\begin{array}{r|l} r & m \\ \hline r & 0 \end{array}$$

Em outras palavras, são os restos possíveis da divisão de qualquer inteiro por m que serão os melhores representantes da classe. Vejamos a seguir um exemplo para esta observação.

Exemplo 2.7. Quando dividimos z, um número inteiro qualquer por $m = 4$, os possíveis restos da divisão inteira de z por 4 são 0, 1, 2 e 3. Portanto, as classes de equivalência determinadas pela relação módulo 4 em $\mathbb{Z}$, são

$$[0],\ [1],\ [2] \text{ e } [3],$$

sendo esses números os "melhores" representantes da classe correspondente.

Desafio!

Escreva as classes de equivalências dos conjuntos quocientes $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ e $\mathbb{Z}/7\mathbb{Z}$, usando as conclusões feitas de como escolher os melhores representantes de cada classe.

Clique aqui para ver a resposta.

Vejamos que, de fato, esses números escolhidos para representantes são os melhores para operar no conjunto quociente $\mathbb{Z}/4\mathbb{Z}$.

Da forma que escolhemos os representantes, temos que $\mathbb{Z}/4\mathbb{Z} = \{[0],\ [1],\ [2],\ [3]\}$, então obtemos os seguintes resultados

$$
\begin{array}{l}
[0] + [1] = [0+1] = [1]; \\
[3] + [3] = [3+3] = [6] = [2], \quad \text{pois} \quad 5 \equiv 1 \pmod 4; \\
[2] + [3] = [2+3] = [5] = [1], \quad \text{pois} \quad 4 \equiv 2 \pmod 4; \\
[0] \cdot [1] = [0 \cdot 1] = [0]; \\
[3] \cdot [2] = [3 \cdot 2] = [6] = [2]; \\
[2] \cdot [2] = [2 \cdot 2] = [4] = [0], \quad \text{pois} \quad 4 \equiv 0 \pmod 4,
\end{array}
$$

e assim por diante. Logo, podemos montar as tabuadas de adição e multiplicação no conjunto $\mathbb{Z}/4\mathbb{Z}$ como ilustradas nas tabelas 2.1 e 2.2.

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

TABELA 2.1: A tabuada da adição em $\mathbb{Z}/4\mathbb{Z}$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

TABELA 2.2: A tabuada da multiplicação em $\mathbb{Z}/4\mathbb{Z}$

Desafio!

Construa as tabuadas da adição e multiplicação nos conjuntos construídos no desafio 2.2.

Clique aqui para ver a resposta.

Observando as tabelas 2.1 e 2.2, podemos concluir algumas propriedades das operações de adição e multiplicação em $\mathbb{Z}/4\mathbb{Z}$.

- A adição e a multiplicação em $\mathbb{Z}/4\mathbb{Z}$ tem a propriedade comutativa?

  Sim, porque as tabuadas são "simétricas" com respeito à diagonal da tabela.

- A adição e a multiplicação em $\mathbb{Z}/4\mathbb{Z}$ tem a propriedade de neutro?

  Sim. Observe que na linha e coluna da classe $[0]$ na adição os elementos são "colados" da respetiva linha e coluna superior e à esquerda. Isso indica que $[0]$ é neutro da adição. Mesma conclusão com a classe $[1]$ no caso da multiplicação.

Mais uma questão: todo elemento tem simétrico ? isto é, para toda classe $[a]$ existe uma classe $[b]$ tal que $[a]$ operado com $[b]$ dá como resultado o neutro?

Note que, para cada elemento de $\mathbb{Z}/4\mathbb{Z}$, encontramos na linha a classe $[0]$. Então o correspondente elemento da coluna que opera com ele é o simétrico da adição. Acostumamos, no lugar de chamar de simétrico aditivo, dizer oposto. Assim, o oposto de $[2]$ é $[2]$ pois $[2]+[2]=[0]$. Na tabela 2.3 está ilustrada com cor verde esta relação de oposto da classe $[2]$.

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

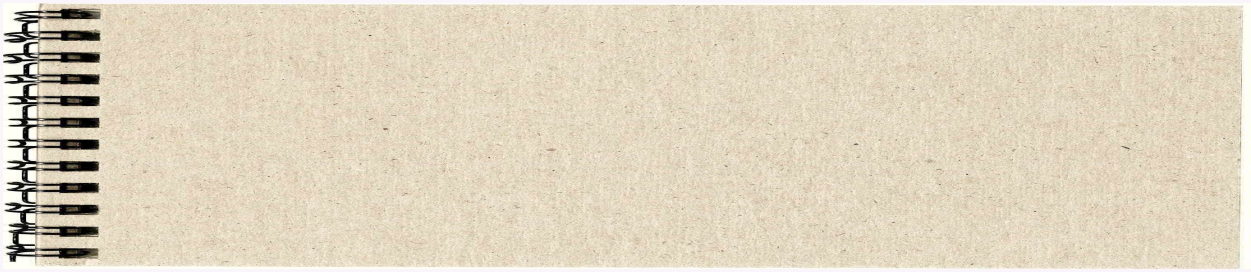
TABELA 2.3: O oposto de $[2]$ é $[2]$ na adição de $\mathbb{Z}/4\mathbb{Z}$

Vamos tirar as mesmas conclusões para a multiplicação?

Observe que, no caso da multiplicação, nem todo elemento $[a] \in \mathbb{Z}/4\mathbb{Z}$ possui simétrico multiplicativo, que denominaremos inverso de $[a]$. Isso você ve na tabuada da multiplicação na linha da classe $[2]$, pois nenhum dos resultados é o neutro multiplicativo $[1]$.

Desafio!

Quais são os elementos de $\mathbb{Z}/4\mathbb{Z}$ que possuem inverso?



Clique aqui para ver a resposta.

2.3 Congruência e Divisibilidade

Você já conhece a brincadeirinha de como usar os restos das divisões de números com aqueles amigos, colegas não muito habituados a usar divisibilidade?

A brincaderia é a seguinte: peça para seu amigo, colega, escolher um número qualquer, inteiro por sinal, pois estamos trabalhando em $\mathbb{Z}$. Vamos chamar de n ao número escolhido. Agora vamos confundir seu coleguinha fazendo algumas contas. Siga a ordem abaixo:

1. Triplique n (obtemos $3n$);
2. Acrescente 6 ao resultado (obtemos $3n + 6$);
3. Triplique o resultado (obtemos $3(3n + 6)$);
4. Some os dígitos do número resultante e me devolva a resposta.

Você aguarda apenas uns segundos e responde: o número resultante é 9. Claro que seu interlocutor vai levantar suspeitas de existência de algum "truque". Vamos explicar porque o resultado é sempre 9 independentemente do número escolhido.

Dos cálculos que pedimos para fazer obtemos que o número x resultante vai ser igual a $3(3n + 6) = 9(n + 2)$, que garante ser um número múltiplo de nove. Agora lembre que os

números múltiplos de nove verificam essa surpreendente propriedade: a soma dos seus dígitos é sempre 9!

Esta e outras propriedades relativas à divisibilidade será o objetivo desta seção. Começamos nosso estudo lembrando que a representação decimal de um número inteiro positivo a é dada por

$$a = a_{n-1}a_{n-2}\cdots a_1a_0,$$

que é a notação correspondente ao número

$$a = a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + \cdots + a_1 10 + a_0, \tag{2.9}$$

com os dígitos $0 \leq a_i \leq 9$ para $i = 0, 1, \ldots, n-1$.

Vamos explorar as propriedades relação de congruência e a representação decimal para concluir os conhecidos **critérios de divisibilidade**. Desta vez de forma fundamentada.

Mostraremos os fundamentos da **prova dos noves**, que é o que motivou a brincadeira no início desta seção.

Teorema 2.5 (Teste de divisibilidade por 9)**.** *Seja $a \in \mathbb{Z}^+$ dado pela sua representação decimal 2.9. Então*

$$a \equiv (a_{n-1} + \cdots + a_0) \pmod 9.$$

E por que o teorema 2.5 é um teste de divisibilidade por 9?

Note que, se $(a_{n-1} + \cdots + a_0)$ é congruente com zero no módulo 9, então, pela propriedade transitiva da relação congruência, teremos que a é congruente com zero módulo 9, o que significa que 9 divide a a.

Na realidade, com o mesmo trabalho, podemos demonstrar um teorema mais geral que expressa a divisivilidade de um número pelos primeiros da lista de primos naturais.

Teorema 2.6. *Seja $a \in \mathbb{Z}$ dado pela sua representação decimal 2.9. Então*

1. $a \equiv a_0 \pmod 2$;
2. $a \equiv a_0 \pmod 5$;
3. $a \equiv 3 = (a_{n-1} + \cdots + a_0) \pmod 3$;
4. $a \equiv (a_{n-1} + \cdots + a_0) \pmod 9$;
5. $a \equiv (a_0 - a_1 + a_2 - a_3 + \cdots) \pmod{11}$;

Demonstração:

Vamos considerar o polinômio cujos monômios têm como coeficientes os dígitos do número a como 2.10

$$p(x) = a_{n-1}x^{n-1} + \cdots + a_1x + a_0. \tag{2.10}$$

Sabemos que $10 \equiv 0 \pmod 2$ pois $2 \mid 10$. Então, pelo teorema 2.3 item 5, temos que

$$a_{n-1}10^{n-1} + \cdots + a_110 + a_0 \equiv a_{n-1}0^{n-1} + \cdots + a_10 + a_0 \pmod 2,$$

ou seja,

$$a \equiv a_0 \pmod 2.$$

Isto prova o item 1.

Como temos $10 \equiv 0 \pmod 5$, a demonstração do item 2 é similar.

Note que também temos que $10 \equiv 1 \pmod 3$, logo, aplicando novamente o teorema 2.3, obtemos

$$a_{n-1}10^{n-1} + \cdots + a_110 + a_0 \equiv a_{n-1}1^{n-1} + \cdots + a_11 + a_0 \pmod 3,$$

o que é equivalente a

$$a \equiv a_{n-1} + \cdots + a_1 + a_0 \pmod 3,$$

o que prova o item 3.

Usando que $10 \equiv 1 \pmod 9$, a demonstração do item 4 procede da mesma maneira.

Do fato de que $10 \equiv -1 \pmod{11}$, concluímos que

$$a_{n-1}10^{n-1} + \cdots + a_110 + a_0 \equiv a_{n-1}(-1)^{n-1} + \cdots + a_1(-1) + a_0 \pmod{11},$$

ou seja,

$$a \equiv a_0 - a_1 + a_2 - \cdots \pmod{11}$$

demonstrando do teorema. ■

Corolario 2.1. *Seja a dado pela representação decimal equarepdecimalint. Então*

1. $2 \mid a$ *se e somente se* $a_0 = 0, 2, 4, 6$ *ou* 8;
2. $5 \mid a$ *se e somente se* $a_0 = 0$ *ou* 5;
3. $3 \mid a$ *se e somente se* $3 \mid a_0 + a_1 + \ldots + a_{n-1}$;
4. $9 \mid a$ *se e somente se* $9 \mid a_0 + a_1 + \ldots + a_{n-1}$;
5. $11 \mid a$ *se e somente se* $11 \mid a_0 - a_1 + a_2 - a_3 + \ldots$

Vejamos um exemplo de como aplicar o teorema 2.6.

Exemplo 2.8. Usando os itens 3 e 4 do corolário 2.1 podemos saber se o número 1487 é divisível por 9 ou não. Veja como fazer:

$$\begin{aligned} 1487 \equiv & (1+4+8+7) \pmod 9 \\ & = ((1+8)+4+7) \pmod 9 \\ & = (9+4+7) \pmod 9 \\ & = (4+7) \pmod 9 \\ & = ((2+2)+7) \pmod 9 \\ & = (2+(2+7)) \pmod 9 \\ & = (2+9) \pmod 9 \\ & = 2 \pmod 9. \end{aligned}$$

Assim, concluímos que $1487 \equiv 2 \pmod 9$, ou seja, não é divisível por 9.

Desafio!

Mostre que o número $2.346.025$ é múltiplo de 11. Anote no caderno.

Clique aqui para ver a resposta.

Estudamos a seguir a divisibilidade pelos números 7 e 13.

Teorema 2.7. *Seja $a = a_r a_{r-1} \cdots a_1 a_0$ a representação decimal do número a. Então*

1. $7 \mid a$ *se e somente se* $7 \mid a_r \cdots a_1 - 2a_0$;
2. $13 \mid a$ *se e somente se* $13 \mid a_r \cdots a_1 - 9a_0$,

onde $a_r \ldots a_1 = \frac{a-a_0}{10} = a_r 10^{r-1} + \ldots + a_2 10 + a_1$.

Vamos ilustrar o teorema 2.7 com alguns exemplos.

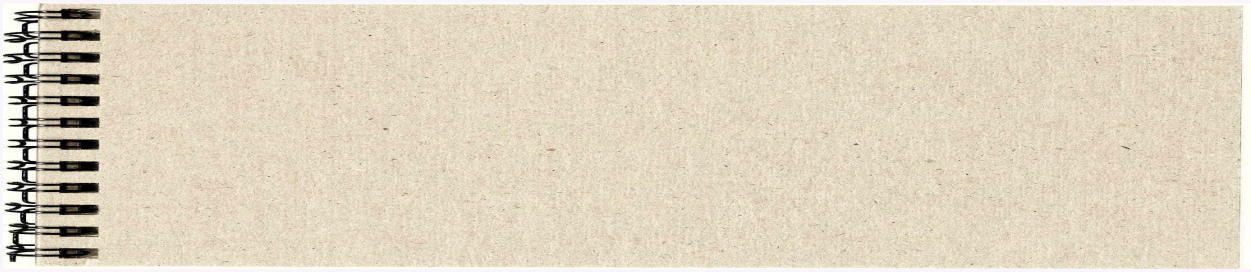
Exemplo 2.9. Vamos mostrar que $7 \mid 2.481$. Pelo teorema 2.7 será verdade se e somente se $7 \mid 248 - 2$, o que é o mesmo que dizer que 7 divide a 246. Agora, usando o teorema 2.7 de novo, temos que 7 teria que dividir a $24 - 12 = 12$, que não é verdadeiro. Então $7 \nmid 2481$.

Outro exemplo usando a prova do 13: queremos mostrar que $13 \mid 12.987$, então, pelo teorema 2.7 é equivalente a que $13 \mid 1.298 - 63$. Por outro lado,$13 \mid 1.235$ se e somente se $13 \mid 123 - 45$ que pela sua vez é equivalente a que $13 \mid 78$, o que é verdadeiro. Assim, temos que $13 \mid 12.987$.

Agora a sua vez de aceitar o desafio:

Desafio!

Mostre que o número 41.405 é múltiplo de 91. Anote no caderno.



Clique aqui para ver a resposta.

Demonstração: (Demonstração de Teorema 2.7)

Seja $c = a_r \cdots a_1$. Temos que $a = 10c + a_0$ e daí $-2a = -20c - 2a_0$. Assim, como

$1 \equiv -20 \pmod 7$, concluímos que segue pelo teorema 2.3 que

$$-2a \equiv c - 2a_0 \pmod 7.$$

Portanto, da hipótese que $7 \mid a$ temos que $7 \mid -2a$ o que é equivalente a $7 \mid c - 2a_0$.

Recíprocamente, de que $MDC(7, -2) = 1$ temos, pelo lema de Euclides que $7 \mid -2a$, ou seja, $7 \mid a$. ■

2.4 Congruências lineares e equações diofantinas lineares.

Imaginemos a seguinte situação: os alunos de matemática da UFU estao rcoletando dinheiro para fazer a festa de colação de grau. Para isso eles estão vendendo rifas de 30 reais e 50 reais correspondentes a diferentes prêmios. Maria leva uma quantidade x de rifas de 30 reais e y de 50 reais, arrecadando com essas rifas um total de 1.240 reais. Quando os colegas de Maria perguntaram quantas rifas ela tinha vendido, infelizmente ela só lembrava que tinha vendido mais de 35 rifas de 30 reais mas não tinha anotado os detalhes da venda, além do erro que cometeu a gráfica de não numerar as folhas de cada rifa.

Como resolver o problema da contabilidade de Maria? Será que ela consegue recuperar esses dados usando matemática?

Façamos uma análise notando que, se não tivesse vendido nenhuma rifa de 30 reais, então deveríamos ter $50y = 1.240$, que não tem uma solução inteira, tipo de solução que estamos procurando, pois 1.240 não é divisível por 50. Então, Maria deve ter vendido alguma rifa de 30 reais. Certo ... mas pode ser que não tenha vendido nenhuma de 50 reais! Porém, a equação $30x = 1.240$ também não tem solução inteira. Portanto estamos procurando soluções inteiras não nulas da equação

$$30x + 50y = 1240. \tag{2.11}$$

Uma equação do tipo (2.11) é chamada de **equação diofantina linear**, onde as soluções procuradas também pertencem ao conjunto dos números inteiros. A definição geral é a seguinte.

Definição 2.3. *Uma equação do tipo*

$$ax + by = c, \tag{2.12}$$

onde a, b e c são inteiros e suas soluções também é chamada de equação diofantina linear.
Em outras palavras, as equacões diofantinas lineares são equações de duas variáves com coeficientes inteiros e com soluções, se existirem, também pertencentes ao conjunto dos números inteiros.

O nome de **equação diofantina** é devido ao matemático Diophantus de Alexandria (por volta de 200 a 284 AC), reconhecido por muitos como o "pai da álgebra" e bem conhecido pelo seu livro *Arithmetica*, um trabalho sobre soluções de equações algébricas e em teoria dos números inteiros. Foi o matemático francés Pierre de Fermat (1601-1665) que estudou uma equação de Diofanto que não tinha sido resolvida e, de acordo com os historiadores, Fermat anotou na margem do livro *Arithmetica* de Diofanto uma suposta demonstração da resolução, referida na atualidade como o **último teorema de Fermat**.

Observação 2.2.

- Nem toda equação do tipo (2.12) tem solução. De fato, tomando a equação $4x + 6y = 21$, notamos que o número $4x + 6y$ é um número par, independentemente dos valores de x e y. Portanto não pode ser igual a um número ímpar. Assim esta equação diofantina não tem solução.
- Geometricamente o par solução $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ de uma equação diofantina são os pontos do plano com coordenadas inteiras da reta de equação $ax + by = c$.

Analisando um pouco mais o observado em 2.2 com respeito à equação $4x + 6y = 21$, vemos que MDC$(4, 6)$ não divide a 21. Este parece ser um fato geral. Com efeito, se temos a equação diofantina linear (2.12) onde d é um divisor comum a a e b, então $d \mid (a \cdot x + b \cdot y)$ para quaisquer $x, y \in \mathbb{Z}$.

Isto é uma condição *necessária* para a obtenção de solução para a equação diofantina linear, ou seja, é necessário que todo divisor comum de a e b tem que ser também divisor de c. É claro que, se isto acontece, então, em particular, o máximo divisor comum de a e b também deve dividir a c.

O teorema a seguir mostra que a condição necessária e também suficiente para que uma

equação diofantina linear tenha solução. Ou seja, só temos soluções para o caso que acabamos de analisar.

Teorema 2.8. *A equação* (2.12) *possui soluções inteiras se e somente se* $d \mid c$*, onde* $d = MDC(a, b)$*. Caso a equação possua uma solução* $x = x_0$*,* $y = y_0$*, então deve possuir mais de uma solução dada por*

$$x = x_0 + \frac{b}{d}t \quad \text{e} \quad y = y_0 - \frac{a}{d}t, \tag{2.13}$$

onde t *é um inteiro qualquer.*

Demonstração: Suponha que a equação (2.12) tenha uma solução $(x, y) \in \mathbb{Z} \times \mathbb{Z}$. Como $d \mid a$ e $d \mid b$, então

$$d \mid (ax + by) = c.$$

Suponha que $d \mid c$. Pelo teorema de Bezout (veja no módulo I), existem inteiros m e n tais que

$$d = am + bn$$

e um inteiro k tal que

$$c = dk.$$

Como temos que $c = ax + by$ então

$$c = dk = (ma + nb)k = a(km) + b(nk).$$

Logo a solução da equação $ax + by = c$ é

$$x_0 = km \quad \text{e} \quad y_0 = kn.$$

Vamos provar que existem mais soluções. Sejam

$$x = x_0 + (b/d)t \quad \text{e} \quad y = y_0 - (a/d)t, \tag{2.14}$$

onde t é um inteiro qualquer. Substituindo na expressão do membro à esquerda de (2.12), obtemos

$$ax + by = a(x_0 + (b/d)t) + b(y_0 - (a/d)t) = ax_0 + by_0 = c,$$

o que mostra que x e y definidos em (2.14) são de fato soluções da equação (2.12). ■

Voltemos à equação da nossa motivação inicial (2.11). Temos que o máximo divisor comum de 30 e 50 é 10, que divide a 1240. Assim a condição necessária e suficiente de existência está verificada. Logo, Maria vai poder recuperar os dados para seus colegas usando o teorema 2.8.

Primeiramente observemos que $10 = 30 \cdot 2 + 50 \cdot (-1)$, correto? Assim, multiplicando esta igualdade por 124, obtemos

$$1240 = 30(2 \cdot 124) + 50(-1 \cdot 124),$$

de onde concluímos que o par $(248, -124)$ é solução do problema. O inconveniente desta solução é que -124 não é uma reposta que Maria está procurando, pois y representa o número de rifas. Portanto tem que ser um número natural. Agora, usando o teorema 2.8, temos ainda a informação que todo par do tipo $(248 + (50/10)t, -124 - (30/10)t)$ é solução da equação (2.11).

Assim, poderíamos escolher $t \in \mathbb{Z}$ de forma que

$$-124 - 3t > 0. \tag{2.15}$$

Então, o problema de Maria tem muitas soluções?

Lembremos que a boleta de rifas de 30 reais excedia o número de 35 rifas. Portanto, com esse dado, temos que

$$248 + 5t > 35,$$

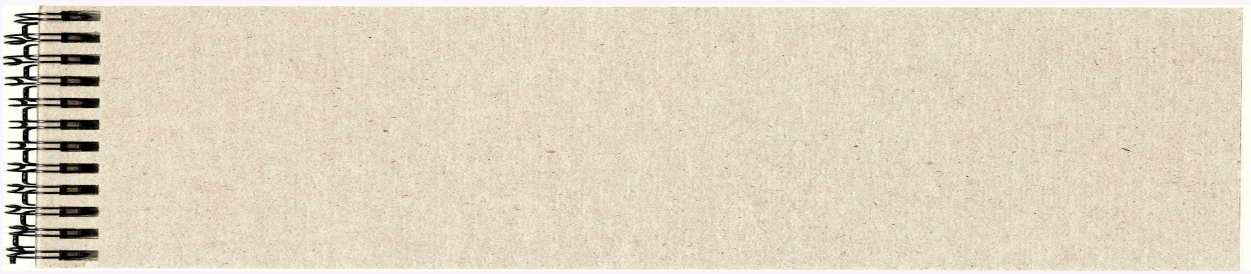
de onde, junto com a conclusão (2.15), chegamos à conclusão de que $y = 2$ e $x = 38$.

Note que, colocando condições "extras" ao problema, podemos obter um única solução. Vejamos outro exemplo para praticarmos a resolução de equações diofantinas.

Exemplo 2.10. *A equação $4x + 6y = 8$ tem infinitas soluções. De fato, como temos $MDC(4, 6) = 2 \mid 8$ e também $4(-1) + 6(1) = 2$, então a soluções particulares da equação são $x_0 = 4.(-1) = -4$ e $y_0 = 4.1 = 4$. Assim, todas as soluções estão dadas por $x = -4 + 3t$ e $y = 4 - 2t$, para qualquer inteiro t.*
Suponha que estamos achando as soluções negativas. Então, devemos ter $3t < 4$ e $2t > 4$ e como t tem que ser inteiro, então não existe (x, y) solução de $4x + 6y = 8$ com x e y simultaneamente negativos.

Desafio!

Resolva a equação diofantina linear $50x + 630y = 10$.



Clique aqui para ver a resposta.

2.4.1 Congruência Linear

Motivamos novamente esta seção com a seguinte situação: Maria (a aluna de matemática da UFU organizando a festa de colação de grau) comprou com parte do dinheiro arrecadado das rifas caixas com lembranças para presentear os 11 professores que confirmaram presença no dia da festa. Maria repartiu as lembranças em saquinhos, misturando os tipos e cada saquinho ficou com a mesma quantidade delas para cada professor, sobrando no total 13 lembranças. Sabendo que o número de caixas compradas por Maria foi menos que uma dezena e que cada caixa trazia 7 lembranças iguais, quantas foram as caixas compradas por Maria?

Para responder a esta pergunta, observemos que, se Maria tinha x caixas de lembrancinhas, então o número total de lembranças é de $7 \cdot x$. Distribuindo as lembranças nos 11 saquinhos e restando 13 lembranças, significa que o resto da divisão inteira de $7 \cdot x$ por 11 é 13. Esta conclusão pode ser expressa em termos de congruência, como

$$7x \equiv 13 \pmod{11},$$

ou, equivalentemente, como temos $13 \equiv 2 \pmod{11}$,

$$7x \equiv 2 \pmod{11}.$$

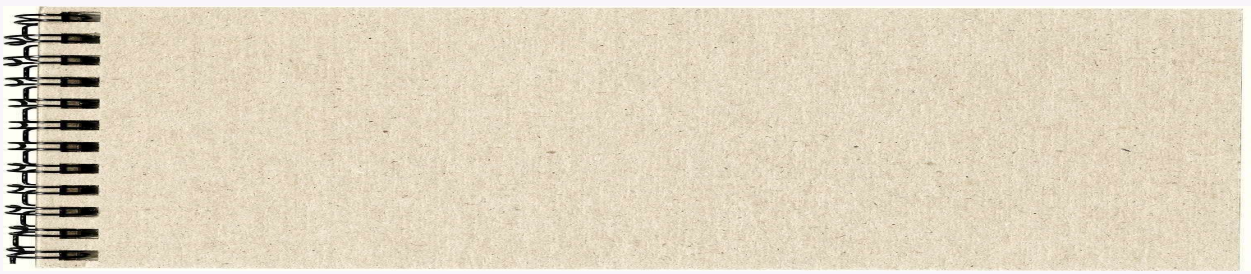
Pela definição de congruência (veja 2.1, pag.93), temos que $11 \mid (7x - 2)$ ou, equivalentemente, $7x - 2 = 11k$ para algum k inteiro. Nossa questão agora é resolver a equação diofantina linear

$$7x - 11k = 2, \tag{2.16}$$

que tem como solução $x = -6 - 11t$, para t um inteiro qualquer. Como o número de caixas é menos que uma dezena, temos que $x = 5$.

Desafio!

Confira que a solução da equação (2.16) é $x = -6 - 11t$ no caderno.



Clique aqui para ver a resposta.

Equações do tipo (2.16) são chamadas de equações de congruência. Este conceito está bem definido a seguir.

Definição 2.4. *Uma equação de congruência da forma*

$$ax \equiv b \pmod{m}, \tag{2.17}$$

onde x é uma variável inteira, é chamada de uma equação de congruência linear.

Note que a forma de resolver a questão das caixas das lembranças de Maria terminou sendo equivalente a resolver uma equação diofantina linear. Isto é o que será destacado como método geral na próxima observação.

Observação 2.3. Note que se x_0 é uma solução para a equação de congruência linear (2.17), então os números inteiros x_i tal que $x_i \equiv x_0 \pmod{m}$ são também soluções da equação (2.17).
Também note que $ax \equiv b \pmod{m}$ é equivalente à equação diofantina linear (2.12) (veja pag. 116). De fato, se existir x solução de (2.12) então temos $ax - my = b$, para algum número inteiro y, de onde o par (x, y) é solução de (2.12). Para mostrar a recíproca desta proposição, basta dar os passos no sentido contrário do raciocínio anterior.

Teorema 2.9. *Sejam $a,\ b$ e m números inteiros, $m > 0$ e $c =$MDC(a, m). Caso c não divida b, então a congruência $ax \equiv b \pmod{m}$ não tem soluções. No caso contrário, temos que $c \mid b$ e como consequência $ax \equiv b \pmod{m}$, que tem exatamente c soluções diferentes módulo m.*

Demonstração: Temos que a equação $ax \equiv b \pmod{m}$ é equivalente a $ax - my = b$ e esta equação não tem solução se c não divide a b. Note também que se $c \mid b$, então temos infinitas soluções dadas por $x = x_0 + \frac{m}{c}(-k)$, com t um número inteiro. Escrevendo $-k = t$, temos $x = x_0 + \frac{m}{c}k$, são soluções da congruência $ax \equiv b \pmod{m}$. Suponha que temos duas soluções que são congruentes no modulo m. Então,

$$x_0 + \tfrac{m}{c}t_1 \equiv x_0 + \tfrac{m}{c}t_2 \pmod{m},$$

de onde obtemos

$$\tfrac{m}{c}t_1 \equiv \tfrac{m}{c}t_2 \pmod{m}.$$

Note que MDC$(m, \frac{m}{c}) = \frac{m}{c}$ e portanto

$$t_1 \equiv t_2 \pmod{c}.$$

Como consequência, obtemos soluções diferentes dadas por $x = x_0 + \frac{m}{c}t$, onde t é tomado no módulo c. ■

Observação 2.4. Note que a demonstração do teorema 2.9 mostra exatamente quais são as soluções da equação de congruência linear $ax \equiv b \pmod{m}$ quando $c =$MDC$(a, m) \mid b$. Sendo x_0 uma solução particular com $0 \leq x_0 < \frac{m}{c}$, estas são

$$x = x_0 + \frac{m}{c}t, \quad \text{com } 0 \leq t \leq c \tag{2.18}$$

Exemplo 2.11. Vamos achar as soluções de $3x \equiv 12 \pmod{6}$. Note que MDC$(3, 6) = 3$ e que $3 \mid 12$. Então temos três soluções que não são congruentes no módulo 6. Usando a equação diofantina equivalente $3x - 6y = 12$, temos que $x_0 = 4$ e portanto as soluções são dadas por $x_1 = 4 \pmod{6}$, $x_1 = 4 + 2 \equiv 0 \pmod{6}$ e $x_2 = 4 + 4 \equiv 2 \pmod{6}$.

Como mencionado anteriormente, a congruência $ax \equiv b \pmod{m}$ tem uma única solução com a condição que MDC$(a, m) = 1$. Isto nos permite definir o que é o inverso modular de um número inteiro como especificamos na definição a seguir.

Estudaremos a seguir as equacões de congruência do ponto de vista das classe de equivalência definidas em $\mathbb{Z}/m\mathbb{Z}$ e utilizaremos as operações definidas nesse conjunto.

Assim, no lugar de resolver a equação de congruência $ax \equiv b \pmod{m}$, vamos resolver a equação em $\mathbb{Z}/m\mathbb{Z}$

$$[a] \cdot [x] = [b], \tag{2.19}$$

onde $\cdot$ é o produto definido em $\mathbb{Z}/m\mathbb{Z}$ (veja 2.2, pag. 104). A ideia é usar a mesma técnica que usamos quando resolvermos a equação $ax = b$, por exemplo, no conjunto dos números reais. O que fazemos neste caso é "passar" a para o outro membro, dividindo para assim obtermos a expressão de x. Na realidade, o que fazemos teoricamente é multiplicar ambos os membros da equação pelo inverso de a, obtendo $a^{-1}(ax) = a^{-1}b$ e como $a^{-1}a = 1$ chegamos a que $x = a^{-1}b$ que é a solução da equação.

Vamos proceder de forma análoga para resolver (2.19). Note que se a não possui inverso multiplicativo, a equação pode não ter soluções ou pode ter mais de uma solução! Vejamos um exemplo.

Exemplo 2.12. Vamos resolver

$$[4] \cdot [x] = [3], \quad \text{em } \mathbb{Z}/5\mathbb{Z}. \tag{2.20}$$

A questão inicial é qual seria, se existir, o simétrico multiplicativo ou inverso de $[4[$ em em $\mathbb{Z}/5\mathbb{Z}$?. De acordo com a definição de inverso, temos que x é o inverso de $[4]$, verifica ser solução de $4x \equiv 1 \pmod 5$, pois temos MDC$(4, 5) = 1$. Uma das soluções é $x = 4$ e, portanto, temos que $[4]$ é o inverso de $[4]$ em $\mathbb{Z}/5\mathbb{Z}$. Portanto, a solução de (2.20) é

$$[x] = [4] \cdot [3] = [4 \cdot 3] = [12] = [2].$$

Exemplo 2.13. A equação $[2] \cdot [x] = [1]$ não tem solução em $\mathbb{Z}/4\mathbb{Z}$, pois o MDC$(2, 4) = 2$ não divide a 1.
Por outro lado, se tentarmos resolver a equação $[2] \cdot [x] = [2]$ temos chances pois MDC$(2, 4) \mid 2$. A curiosidade desta equação é que tem mais de uma solução no conjunto $\mathbb{Z}/4\mathbb{Z}$. Com efeito, claramente $[x] = [1]$ é solução. Mas também temos que $[x] = [3]$ é solução, pois $[3]$ é inverso de $[2]$ no conjunto $\mathbb{Z}/4\mathbb{Z}$.

O exemplo 2.13 mostrou que, para um número natural m qualquer, nem todo elemento de $\mathbb{Z}/m\mathbb{Z}$ possui inverso.

Vamos caracterizar os elementos que possuem inverso em $\mathbb{Z}/m\mathbb{Z}$. Notamos nos exemplos que se $[a] \in \mathbb{Z}/m\mathbb{Z}$, então $[a]$ possui inverso se $[1] = [a] \cdot [x] = [ax]$, o que equivale a dizer que $a \cdot x \equiv 1 \pmod m$. Assim, pelo teorema 2.9 sabemos que esta última equação de congruência tem solução se e somente se MDC(a, m) divide a 1, ou seja, devemos ter necessariamente MDC$(a, m) = 1$. Como conclusão, temos a seguinte proposição.

Proposição 2.2. *Dado m inteiro positivo. O elemento $[a] \in \mathbb{Z}/m\mathbb{Z}$ possui inverso se e somente se MDC$(a, m) = 1$.*

Exemplo 2.14.

1. Os únicos elementos de $\mathbb{Z}/6\mathbb{Z}$ que possuem inverso multiplicativo são $[1]$ e $[5]$, já que 1 e 5 são os únicos números inteiros entre 0 e 5 que verificam MDC$(a, 6) = 1$.

2. Todos os elementos de $\mathbb{Z}/5\mathbb{Z}$ têm inverso multiplicativo, pois para todo a entre 0 e 4 temos MDC$(a, 5) = 1$.

Note que, no item 2 do exemplo 2.14, o fato de 5 ser um número primo tem a ver com que no conjunto $\mathbb{Z}/5\mathbb{Z}$ todos os elementos possuem inverso. Ou seja, temos a seguinte proposição.

Proposição 2.3. *Todo elemento de $\mathbb{Z}/p\mathbb{Z}$, com p número primo, possui inverso.*

Demonstração: Por ser p um número primo, os únicos divisores positivos de p são 1 e p. Portanto, se a é um número inteiro tal que $1 \leq a \leq p-1$, o único divisor positivo comum a a e p é 1. Isto mostrou que $\mathrm{MDC}(a,p) = 1$ e dessa forma todos os elementos de $\mathbb{Z}/p\mathbb{Z}$ possuem inverso. ■

Outra propriedade imediata que surge da proposição 2.2 é que $[0] \in \mathbb{Z}/m\mathbb{Z}$ não possui inverso para nenhum $m \geq 2$, porque tem-se que $[0] \cdot [x] = [0] \neq [1]$ para todo $x \in \mathbb{Z}/m\mathbb{Z}$.

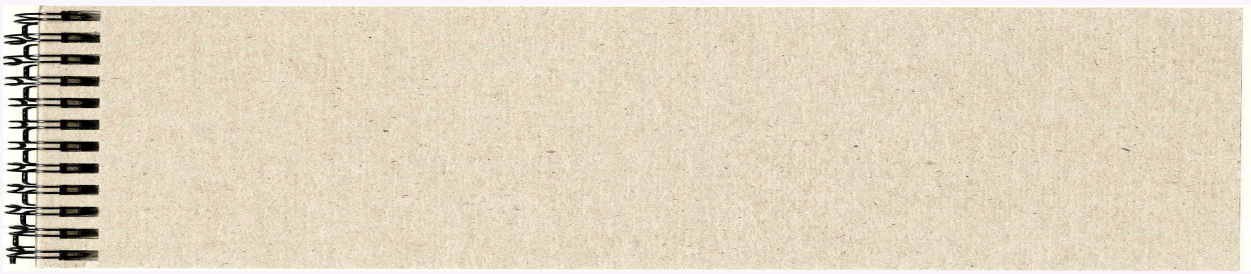
Para o caso em que m não é primo, vamos analisar quais são aqueles $[a]$ que possuem inverso em $\mathbb{Z}/m\mathbb{Z}$. Do fato de que m não é primo devem existir inteiros positivos a e b com $1 < a < m$ e $1 < b < m$ menores que m tais que $m = ab$. Isto significa que a e b são números diferentes de 1, menores que m com MDC$(a,m) \neq 1$ e MDC$(b,m) \neq 1$. Portanto $[a]$ e $[b]$ não possuem inversos em $\mathbb{Z}/m\mathbb{Z}$.

Note também que, usando a conclusão da observação 2.4, obtém-se a seguinte proposição:

Proposição 2.4. *Dada a equação $[a] \cdot [x] = [b]$ em $\mathbb{Z}/m\mathbb{Z}$, onde $c =$MDC$(a,m) \mid b$. Então, se x_0 é uma solução $0 \leq x_0 < \frac{m}{c}$, as outras soluções são dadas por 2.18.*

Desafio!

Escreva todas as soluções da equação $[5] \cdot [x] = [4]$ em $\mathbb{Z}/14\mathbb{Z}$ no caderno.



Clique aqui para ver a resposta.

Aplicação: O teorema chinês do resto

Encontrar um número inteiro tal que a divisão inteira por 3, dá como resto 2, a divisão inteira por 5, dá como resto 3 e por 7 o resto 2.

No século III, o matemático chino Sun-Tzi queria conhecer este número. Em homenagem a ele e outros matemáticos chineses, como Lin Hiu (siglo III), Yang Hui (siglo XI) e Chon Huo (siglo XIII), que aportaram soluções a os *sistemas de congruências* lineares, o teorema é conhecido como o *Teorema Chinês do Resto*.

Os sistemas de congruências lineares são do tipo

$$\begin{cases} x & \equiv & a_1 & \pmod{m_1} \\ x & \equiv & a_2 & \pmod{m_2} \\ & \cdots & & \\ x & \equiv & a_k & \pmod{m_k} \end{cases}$$

O teorema chinês do resto afirma que se m_i, $i = 1, \cdots k$ são números inteiros positivos, coprimos dois a dois, o sistema tem uma única solução em $\mathbb{Z}/m\mathbb{Z}$, onde $m = m_1 \cdot m_2 \cdots m_k$.

Para construir a solução simultânea, primeiro definimos

$$M_i = \frac{m}{m_i},\ i = 1, \cdots, k,$$

que representa o produto de todos os módulos, exceto m_i. Pelo teorema, sabemos que os m_i não têm fator em comum maior que 1 com o restantes m_j. Logo, existe um número inteiro y_i, que é o inverso de M_i em $\mathbb{Z}/m_i\mathbb{Z}$. Portanto,

$$M_i \cdot y_i \equiv 1 \pmod{m_i}.$$

Assim,

$$x \equiv a_1 M_1 y_1 + \cdots + a_k M_k y_k, \pmod{m}$$

é a solução procurada.

No caso do problema proposto, temos que $[2]$ é o inverso de [2] em $\mathbb{Z}/3\mathbb{Z}$, $[3]$ é inverso de $[1]$ em $\mathbb{Z}/5\mathbb{Z}$ e $[1]$ é inverso de $[1]$ em $\mathbb{Z}/7\mathbb{Z}$ módulo 7 portanto

$$x \equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \pmod{105}$$

e temos $233 \equiv 23 \pmod{105}$. Portanto, 23 é o menor número inteiro que na divisão inteira de 23 por 3, 5 e 7, se obtém restos respectivos de 2, 3 e 2.

2.5 Respostas aos desafios do módulo 2

- Desafio da página 93.

  1. $1 \equiv -3 \pmod 4$ porque $4 \mid (1-(-3)) = 4$
  2. $25 \not\equiv 2 \pmod 4$ porque $4 \nmid (25-2) = 23$

- Desafio da página 100.

  De que $a \equiv -1 \pmod 7$, $b \equiv 6 \pmod 7$ e que $c \equiv 3 \pmod 7$, usando o teorema 2.3, item 1, obtemos, somando membro a membro, as três congruências,

  $$a+b+c \equiv -1+6+3 \pmod 7,$$

  ou seja,

  $$a+b+c \equiv 8 \pmod 7.$$

  Como temos $8 \equiv 1 \pmod 7$, pela transitividade da relação $\equiv$ obtemos que

  $$a+b+c \equiv 1 \pmod 7$$

  o que significa que o resto da divisão é 1.

- Desafio da página 100.

  Temos que $7 \equiv 4 \pmod 3$ porque $3 \mid (7-4) = 3$. Usando o item 4 do teorema 2.3 $7^{25} \equiv 4^{25} \pmod 3$. Por outro lado, $4 \equiv 1 \pmod 3$ de onde, $4^{25} \equiv 1 \pmod 3$. Pela propriedade transitiva da relação de congruência ($\equiv$), obtemos que $7^{25} \equiv 1 \pmod 3$. Ou seja, $3 \mid (7^{25}-1)$ e daí para algum q temos $7^{25}-1 = 3q$ ou equivalentemente , $7^{25} = 3q+1$. Como $0 \leq r < 3$, 1 é o resto da divisão inteira de 7^{25} por 3.

- Desafio da página 103.

  Note que $23 \equiv 3 \pmod 4$. Assim, calculando as potências de 3

  $$\begin{aligned} 3^0 = 1 &\equiv 1 \pmod 4 \\ 3^1 = 3 &\equiv 3 \pmod 4 \\ 3^2 = 9 &\equiv 1 \pmod 4 \\ 3^3 = 27 &\equiv 3 \pmod 4 \end{aligned}$$

  Assim, concluímos que para todo k temos

  $$3^{2k+1} \equiv 3 \pmod 4.$$

  Como 71.355 é ímpar, então o resto da divisão inteira de $23^{71.355}$ por 3 é 1.

- Desafio da página 107. Note que $89 \equiv 1 \pmod{44}$ e que $55 \equiv 11 \pmod{44}$. Assim, usando propriedades da congruência (soma e multiplicação do teorema 2.3), obtemos que

  $$[89]+[55] = [1]+[11] = [12],$$

$$[89] \cdot [55] = [1] \cdot [11] = [11].$$

Note que usamos os restos da divisão inteira como melhores representantes!

- Desafio da página 107.

$\mathbb{Z}/2\mathbb{Z} = \{[0],\ [1]\};$

$\mathbb{Z}/3\mathbb{Z} = \{[0],\ [1],\ [2]\};$

$\mathbb{Z}/5\mathbb{Z} = \{[0],\ [1],\ [2],\ [3],\ [4]\};$

$\mathbb{Z}/7\mathbb{Z} = \{[0],\ [1],\ [2],\ [3],\ [4],\ [5], [6]\};$

- Desafio da página 108.

As tabelas das operações de adição e multiplicação em $\mathbb{Z}/2\mathbb{Z}$ são as seguintes:

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

As tabelas das operações de adição e multiplicação em $\mathbb{Z}/3\mathbb{Z}$ são as seguintes:

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

$\cdot$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

Tente as outras quatro tabuadas pela sua conta! Consulte o tutor por qualquer dúvida!

- Desafio da página 110.

  São as classes $[1]$ e $[3]$ cujos inversos são eles mesmos.

- Desafio da página 113.

  Pelo teorema 2.6 temos que

$$2.346.030 \equiv \underbrace{(2-3+4-6+0-2+5)}_{0} \pmod{11}$$

  de onde $11 \mid 2.346.025$, ou, equivalentemente, $2.346.025$ é múltiplo de 11.

- Desafio da página 114.

  Note que 91 é o produto de $7 \cdot 13$. Assim mostrando que $7 \mid 41.405$ e $13 \mid 41.405$, então estamos monstrando que 41.405 é múltiplo de 91. Usando o teorema 2.7, temos que $7 \mid 41.405$ se e somente se $7 \mid 4140 - 2 \cdot 5 = 4.130$ e, usando novamente o teorema 2.7, temos que $7 \mid 4130$ se e somente se verificam as seguintes afirmações: $7 \mid 413 - 2 \cdot 0 = 413$ e $7 \mid 41 - 2 \cdot 3 = 35 = 5 \cdot 7$ que é verdadeiro.

Por outro lado, usando a prova do 13, temos que $13 \mid 41.405$ se e somente se

$$13 \mid 4.140 - 9 \cdot 5 = 4.095$$

que é equivalente a que $13 \mid 409 - 9 \cdot 5 = 364$, e, pela sua vez, equivalente a que $13 \mid 36 - 9 \cdot 4$ que é verdadeiro.

- Desafio da página 118.

  A equação $50x + 630y = 10$ tem solução, pois o $\mathrm{MDC}(50, 630) = 10$ que divide a 10, termo independente da equação. Como podemos escrever

  $$50 \cdot (-25) + 630 \cdot 2 = 10,$$

  (esta afirmação constitui outro desafio para você!) então $(x, y) = (-25, 2)$ é uma solução. Usando o teorema 2.8, obtemos o conjunto solução cujos elementos são da forma

  $$(-25 + 63t, 2 - 5t),\ t \text{ número inteiro.}$$

- Desafio da página 119.

  A equação

  $$7x - 11k = 2,$$

  tem solução pois $\mathrm{MDC}(7, 11) = 1$ que divide a 2. Como temos

  $$1 = 7(-3) - 11(-2),$$

  (prove isto como mais um desafio!) então

  $$2 = 7(-6) - 11(-4).$$

  Usando o teorema 2.8, obtemos que $x = -6 - 11t$, como queríamos provar.

- Desafio da página 123.

  $[5] \cdot [x] = [4]$. Sendo $[3]$ o inverso de $[5]$ (prove!) então $[x] = [3] \cdot [4] = [12]$.

Módulo 3
O conjunto dos Números Racionais

Introdução

No término do módulo III, o aluno estará familiarizado como os seguintes conceitos:

1. O conjunto dos números racionais.

2. Números racionais decimais.

3. A noção de enumeração no Conjunto dos Números Racionais.

3.1 O Conjunto dos Números Racionais

Intuitivamente pensamos os números racionais como quociente de dois números inteiros m e n com $n \neq 0$. Ou seja, uma definição formal seria que o número $\frac{m}{n}$ é um número racional.

A questão é quantas frações do tipo $\frac{m}{n}$ representam o mesmo cálculo, como por exemplo $\frac{1}{4}$ e $\frac{2}{8}$. Foi assim que surgiu a necessidade de uma definição precisa que identifique, por exemplo, os números $\frac{1}{4}$ e $\frac{2}{8}$.

Uma forma de apresentar os números racionais é considerando o conjunto

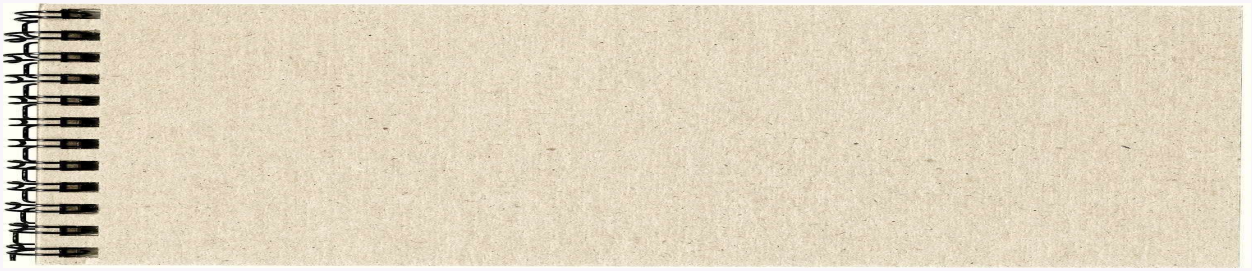
$$\mathbb{Z} \times (\mathbb{Z} - \{0\}) = \{(m, n) : \ m, \ n \in \mathbb{Z}, \ n \neq 0\}.$$

Estabelecemos uma relação de equivalência (veja no Módulo I a definição, 1.8 pg. 24) entre os elementos deste conjunto da seguinte maneira:

Definição 3.1. *Para todo* (a, b) *e* $(c, d) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$*, dizemos que* (a, b) *é equivalente a* (c, d) *se e somente se* $ad = bc$.

Desafio!

Mostre que, de fato, a relação definida em 3.1 é uma relação de equivalência.



Clique aqui para ver a resposta.

Desta forma o conjunto quociente (veja no módulo 1 a definição1.10, pg.25) determinado em $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ pela relação de equivalência 3.1 é o conjunto das classes de equivalência determinada, como mostra a figura 3.1

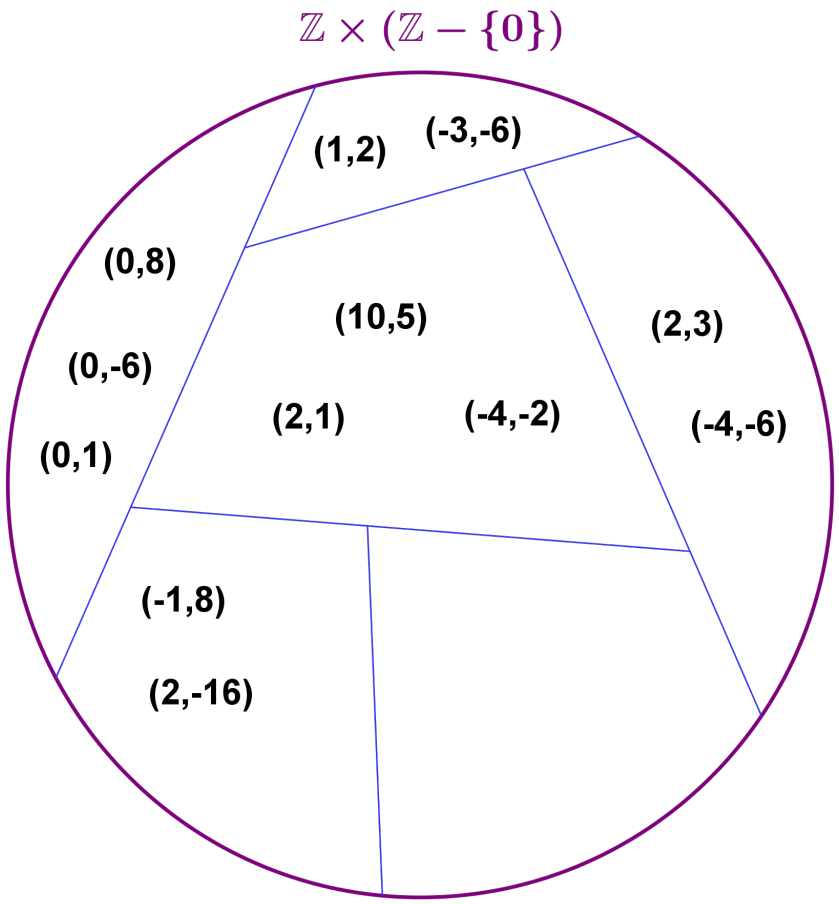


FIGURA 3.1: A partição de $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ em classes de equivalências.

Assim faz sentido fazer a seguinte definição do *Conjunto dos Números Racionais*.

Definição 3.2. *O conjunto dos números racionais denotado por $\mathbb{Q}$ é o conjunto das classes de equivalência determinada pela relação 3.1.*

3.1.1 As operações em $\mathbb{Q}$

A partir da definição formal de número racional, vamos definir operações em $\mathbb{Q}$. Vamos definir estas operações de forma que sejam coerentes com nossas expectativas: o resultado de operar frações como "classe de equivalência" seja igual a de operar frações como fazíamos na escola.

Para efetuar qualquer operação no conjunto $\mathbb{Q}$ iremos sempre escolher um representante da classe. A melhor escolha sempre é o representante irredutível, que será definido posteriormente. Mas qualquer outro da classe pode ser utilizado para calcular o resultado de operar dois racionais.

Primeiramente definimos *Adição de Números Racionais*

Definição 3.3. *Dados $q_1 = \frac{a}{b},\ q_2 = \frac{c}{d} \in \mathbb{Q}$ definimos $q_1 + q_2$ como a classe do representante $(ad + bc, bd)$.*
Em outras palavras e usando a outra notação para a classe, temos que

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)]. \tag{3.1}$$

A pergunta agora é: a operação de adição (3.1) está bem definida?
Como assim?
"Definida" no sentido de que o resultado não depende do representante utilizado de cada classe.

A resposta a esta pergunta está na seguinte proposição na qual veremos que, independentemente do representante que escolhemos para somar, o resultado é um par de inteiros da mesma classe, como mostra a proposição 3.1 a seguir.

Proposição 3.1. *Dados os racionais* $q_1 = [(a, b)]$ *e* $q_2 = [(c, d)]$ *e os pares de números inteiros* (a_1, b_1) *e* (c_1, d_1) *tais que*

$$(a, b) \sim (a_1, b_1) \text{ e } (c, d) \sim (c_1, d_1), \tag{3.2}$$

então temos

$$(a, b) + (c, d) \sim (a_1, b_1) + (c_1, d_1).$$

Demonstração: De fato, da equivalência (3.2) temos as seguintes igualdades:

$$ab_1 = ba_1 \text{ e } cd_1 = dc_1, \tag{3.3}$$

e queremos demonstrar que

$$(ad + bc, bd) \sim (a_1d_1 + b_1c_1, b_1d_1). \tag{3.4}$$

Aplicando a definição da relação de equivalência (3.1) teriamos que provar que

$$(ad + bc)b_1d_1 = bd(a_1d_1 + b_1c_1).$$

Vamos aplicar a distributiva no membro à esquerda da igualdade acima e depois de operar mostrar que é exatamente o membro da direita da igualdade.

$$\begin{array}{rcll} (ad + bc)b_1d_1 & = & adb_1d_1 + bcb_1d_1 & \\ & = & (ab_1)(dd_1) + (bb_1)(cd_1) & \text{associando;} \\ & = & (ba_1)(dd_1) + (bb_1)(dc_1) & \text{usando (3.3);} \\ & = & bd(a_1d_1) + bd(b_1c_1) & \text{associando;} \\ & = & bd(a_1d_1 + b_1c_1) & \text{usando distributiva.} \end{array}$$

Portanto a igualdade (3.4) é verdadeira e também a proposição. ■

Da mesma maneira vamos definir multiplicação de racionais de forma que o resultado independa do representante da classe.

Definição 3.4. *Dados* $q_1 = \frac{a}{b},\ q_2 = \frac{c}{d} \in \mathbb{Q}$ *definimos* $q_1 + q_2$ *como a classe do representante* (ac, bd).
Em outras palavras e usando a outra notação para a classe, temos que

$$[(a, b)] \cdot [(c, d)] = [(ac, bd)]. \tag{3.5}$$

Como na proposição 3.1 vamos mostrar que o resultado da operação não depende do representante utilizado.

Proposição 3.2. *Dados os racionais* $q_1 = [(a, b)]$ *e* $q_2 = [(c, d)]$ *e os pares de números inteiros* (a_1, b_1) *e* (c_1, d_1) *tais que*

$$(a, b) \sim (a_1, b_1) \text{ e } (c, d) \sim (c_1, d_1), \tag{3.6}$$

então temos

$$(a, b) \cdot (c, d) \sim (a_1, b_1) \cdot (c_1, d_1).$$

Demonstração: Como na proposição 3.1 queremos provar que

$$(ac, bd) \sim (a_1c_1, b_1d_1). \tag{3.7}$$

o que significa pela definição (3.1) que

$$(ac)(b_1d_1) = (bd)(a_1c_1). \tag{3.8}$$

Usando a equivalência (3.6) temos que

$$ab_1 = a_1b \text{ e } cd_1 = dc_1,$$

de onde, multiplicando ambas as igualdades membro a membro, obtém-se

$$(ab_1)(cd_1) = (a_1b)(dc_1),$$

que é a mesma expressão que (3.8) a menos de comutando e associando os elementos do produto obtido. ■

Da mesma forma que no módulo 2 escolhemos os "melhores representantes" da classe de equivalência para facilitar as operações em $\mathbb{Z}/m\mathbb{Z}$, aqui vamos também escolher o melhor representante para facilitar as operações definidas.

A seguinte proposição tem a ver justamente com a melhor representação da classe.

Proposição 3.3. *Todo número racional* r *pode ser unicamente representado por uma fração* $\frac{m}{n}$ *tal que* $n > 0$ *e* $\mathrm{MDC}(m, n) = 1$.

Demonstração: Note que vamos mostrar existência e unicidade da fração $\frac{m}{n}$ que verifica duas condições: denominador positivo, numerador e denominador coprimos.

Seja $\frac{p}{q}$ um representante qualquer de r. Podemos tomar esse representante de forma que $q > 0$. Isto pelo fato de que se $q < 0$, tomariamos como representante $\frac{-p}{-q}$, que possui denominador positivo.

Seja $d = \mathrm{MDC}(p, q)$. Então existem m e n inteiros tais que $p = md$ e $q = nd$ com a propriedade que $n > 0$ e $\mathrm{MDC}(m, n) = 1$ (veja módulo 1, a seção 1.7, 1.12, pg.67). Isto provou existência.

Vamos mostrar unicidade, supondo que existe $\frac{m_1}{n_1}$, outro representante de r com $n_1 > 0$ e $\mathrm{MDC}(m_1, n_1) = 1$. Temos que (m, n) e (m_1, n_1) são equivalentes e daí

$$mn_1 = m_1 n. \tag{3.9}$$

Da equação (3.9) temos que $m \mid m_1 n$ e como $\mathrm{MDC}(m, n) = 1$, pelo Lema de Euclides (veja 1.5 68) concluímos que

$$m \mid m_1. \tag{3.10}$$

Da equação (3.9) também concluímos que $m_1 \mid mn_1$. Como temos que $\mathrm{MDC}(m_1, n_1) = 1$, entao $m_1 \mid m$, e que, comparada com (3.10), concluímos que $m = m_1$.

Com os mesmos argumentos obtemos que $n = n_1$ o que finaliza a demonstração da unicidade e da proposição.

Notação 3.1. *Denotaremos a classe do representante irredutível (m, n) da forma $[(m, n)]$ ou $\frac{m}{n}$, ou seja,*

$$\frac{m}{n} = [(m, n)] = \{(a, b) \in \mathbb{Z} \times (\mathbb{Z} - \{0\}), (a, b) \sim (m, n)\}$$

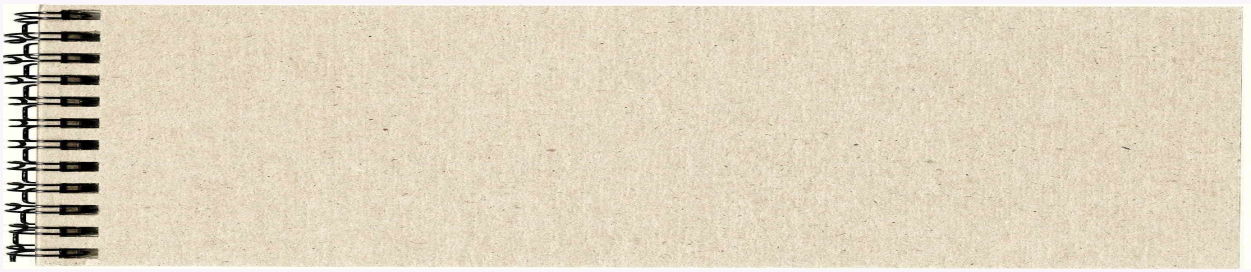
Denominamos a classe $[(m, n)]$ de racional irredutível ou fração irredutível e denotamos $r = \dfrac{m}{n}$.

Observamos que as frações $\frac{1}{2}$ e $\frac{-3}{-6}$ representam **um** número racional por ser equivalentes. Vamos escolher como *representante irredutível* da classe ao par (a, b) cujo $\mathrm{MDC}(a, b) = 1$. No nosso exemplo da classe $\{(1, 2),\ (-3, -6), ...\}$, o representante irredutível é o par $(1, 2)$.

A forma que ensinamos na escola sobre como obter a fração irredutível de uma outra fração, é dividindo ambos, numerador e denominador, pelo MDC desses números. Por exemplo, falando em representante da classe, no caso do representante $(-3, -6)$, como temos $\mathrm{MDC}(-3, -6) = -3$, então o representante irredutível é $(-3/-3, -6/-3) = (1, 2)$.

Desafio!

Encontre os representantes irredutíveis para representar as classes $[(-240, 12)]$, $[(-890, -355)]$ e $[(5.003, 1.110)]$.



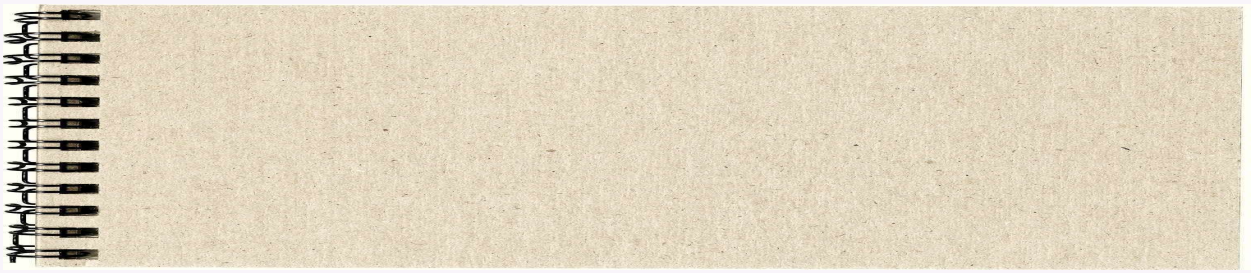
Clique aqui para ver a resposta.

As frações irredutíveis satisfazem uma propiedade importante, que é muito usada desde a época da escola.

Propriedade 3.1. *Seja $\frac{a}{b}$ uma fração irredutível e $\frac{a}{b} = \frac{c}{d}$. Então c é múltiplo de a e d é múltiplo de b. Isto é, existe um número inteiro m tal que $c = a \cdot m$ e $d = b \cdot m$.*

Desafio!

Demonstre a propriedade 3.1 das frações irredutíveis. Anote a prova no caderno.



Clique aqui para ver a resposta.

Em seguida, vamos enunciar algumas propriedades das operações em $\mathbb{Q}$, assim como estabelecer uma relação de ordem neste conjunto.

A adição e a multiplicação definidas em $\mathbb{Q}$ (veja 3.3 em pg. 131 e 3.4 em pg.132) verificam as propriedades usuais da soma de inteiros:

1. Associativa:

$$(\frac{a}{b} + \frac{c}{d}) + \frac{f}{g} = \frac{a}{b} + (\frac{c}{d} + \frac{f}{g}).$$

2. Comutativa
$$\frac{a}{b}+\frac{c}{d}=\frac{c}{d}+\frac{a}{b}.$$

3. Existência e unicidade de neutro.

   - No caso da adição o neutro é o número racional $\frac{0}{1}$. De fato, usando que o número racional $\frac{0}{1}$ é igual a $\frac{0}{q}$, temos que para qualquer número racional $r=\frac{p}{q}$ se verifica
   $$\frac{p}{q}+\frac{0}{q}=\frac{p+0}{q}=r.$$
   - Para a multiplicação o neutro é o número racional $\frac{1}{1}=1$, já que, para qualquer número racional $r=\frac{p}{q}$, temos
   $$\frac{p}{q}\cdot\frac{1}{1}=\frac{p\cdot 1}{q\cdot 1}=r.$$
   - Existência e unicidade do simétrico r' para cada número racional r.
   - No caso da adição, dado $r=\frac{p}{q}$, com $q>0$, tem como simétrico o número racional $r'=\frac{-p}{q}$, onde $-p$ é o oposto de p (veja proposição 1.3 no módulo I, equação (1.18), pg. 44) porque
   $$r+r'=\frac{p}{q}+\frac{-p}{q}=\frac{p+(-p)}{q}=\frac{0}{q}=\frac{0}{1},$$
   ou seja, dá como resultado o neutro da adição. Como no caso do conjunto dos inteiros ao simétrico aditivo, r', do número racional r o chamamos de oposto de r e denotamos por $-r$.
   - Para a multiplicação, dado $r=\frac{p}{q}$ com $p\neq 0$, tem como simétrico o número racional $r''=\frac{q}{p}$ pois
   $$r\cdot r''=\frac{p}{q}\cdot\frac{q}{p}=\frac{p\cdot q}{q\cdot p}=\frac{1}{1},$$
   onde $\frac{1}{1}$ é neutro da multiplicação. Ao simétrico multiplicativo, r'', do número racional r o chamamos de inverso de r e denotamos por r^{-1} ou $1/r$. Note que, o número racional $\frac{0}{1}$ não possui inverso.

Para completar a lista de propriedades temos a seguinte propriedade, que relaciona a adição e a multiplicação.

Propriedade 3.2 (Propriedade distributiva da multiplicação com respeito à adição)**.** Para quaisquer números racionais $r,\ s$ e t verifica-se
$$\frac{a}{b}\cdot(\frac{c}{d}+\frac{f}{g})=\frac{a}{b}\cdot\frac{c}{d}+\frac{a}{b}\cdot\frac{f}{g}.$$

Observação 3.1. Algumas observações e notações que iremos usar.

- Existe uma bijeção entre o subconjunto dos números racionais definido por

$$S = \{r = \tfrac{a}{1},\ a \in \mathbb{Z}\} \tag{3.11}$$

  e o conjunto dos números inteiros. De fato, a bijeção vem definida "naturalmente" como $f : \mathbb{N} \to S,\ f(a) = \frac{a}{1}$.

  Por essa razão, denotamos o número racional $\frac{a}{1}$ como a sua imagem por esta bijeção, isto é, denotamos $\frac{a}{1}$ com a.

- Note que o número racional $\frac{4}{2} = \frac{2}{1} = 2$. Ou seja, para estabelecer a bijeção f usamos o número racional irredutível.

- Note que os neutros da adição e multiplicação em $\mathbb{Q}$ são elementos do conjunto S definido em (3.11). Portanto, pela notação combinada temos que $\frac{0}{1} = 0$ e $\frac{1}{1} = 1$.

3.1.2 Relação de ordem em $\mathbb{Q}$

Vamos definir uma relação de ordem no conjunto $\mathbb{Q}$. Veremos que esta relação de ordem (veja no módulo I, propriedade 1.4, pg. 46) verifica as mesmas propriedades de tricotomia e monotonia da mesma forma que são verificadas pela relação de ordem em $\mathbb{Z}$. (veja no módulo I, propriedade 1.2, pg.37.)

Definição 3.5. *Dados os números racionais $r = \frac{a}{b}$ e $s = \frac{c}{d}$. Diz-se que $r > s$, ou equivalentemente,*

$$\tfrac{a}{b} > \tfrac{c}{d} \text{ se e somente se } a \cdot d > b \cdot c \tag{3.12}$$

Diz-se que $s < r$ se e somente se $r > s$
Diz-se que $r \geq s$ se e somente se $r > s$ ou $r = s$.

3

Observação 3.2. O número racional irredutível $\frac{a}{b}$ é maior que zero se e somente se $\frac{a}{b} > \frac{0}{1}$. Logo, da definição 3.5 devemos ter $a \cdot 1 > b \cdot 0$, ou seja, $a > 0$. Observe que, neste caso, por ser r irredutível, também temos $b > 0$.

Exemplo 3.1. O número racional $\frac{5}{9}$ é maior que $\frac{3}{11}$ pois $5 \cdot 11 > 3 \cdot 9$. Da mesma maneira, $\frac{-3}{11}$ é maior que $\frac{-5}{9}$ pois $-3 \cdot 9 > -5 \cdot 11$.
Note que neste exemplo os números racionais $\frac{5}{9}$ e $\frac{-5}{9}$ são opostos tanto como o são $\frac{3}{11}$ e $\frac{-3}{11}$. Também observe que a relação de ordem entre $\frac{5}{9}$ e $\frac{3}{11}$ há troca de ordem entre os seus respectivos opostos.

Propriedades 3.1 (Propriedades da relação de ordem em $\mathbb{Q}$)**.** *A relação $>$ é uma relação de ordem. Além disso, verificam-se as propriedades de tricotomia e monotonia.*

Vamos demonstrar a propriedade transitiva de 3.1. As outras propriedades são para o próximo desafio.

Demonstração: Sejam $r = \frac{a}{b},\ s = \frac{c}{d}$ e $t = \frac{f}{g}$ números racionais irredutíveis. Pela definição (3.12) temos que

$$\frac{a}{b} > \frac{c}{d} \quad \text{se e somente se} \quad ad > bc \tag{3.13}$$

e também

$$\frac{c}{d} > \frac{f}{g} \quad \text{se e somente se} \quad cg > df. \tag{3.14}$$

Multipliquemos a desigualdade (3.13) pelo número positivo g e a (3.14) pelo número positivo b. Usando a monotonia no conjunto $\mathbb{Z}$ (veja no módulo I, o item 2.3 da propriedade 1.4, pg. 46), obtém-se

$$adg > bcg \text{ e } bcg > bfd.$$

Assim, pela propriedade transitiva da relação de ordem em $\mathbb{Z}$ (veja no módulo I, o item 1 da propriedade 1.4, pg. 46), concluímos que

$$adg > bfd.$$

Usando novamente a propriedade de monotonia em $\mathbb{Z}$ nesta última desigualdade, e sendo $d > 0$, chegamos a que

$$ag > bf \text{ que equivale a dizer que } \frac{a}{b} > \frac{f}{g},$$

como queríamos demonstrar. ■

Desafio!

Demonstre a propriedade de tricotomia da relação de ordem em $\mathbb{Q}$.

Clique aqui para ver a resposta.

Observação 3.3.

- O conjunto dos números racionais juntos com suas duas operações forma um **Corpo** AVA.
- Como a relação de ordem $\geq$ verifica as propriedades 3.1 o conjunto dos números racionais, com suas operações e a relação de ordem é um **Corpo Ordenado** AVA .

Proposição 3.4 (Propriedade Arquimediana do Corpo Ordenado $\mathbb{Q}$)**.** *Sejam r e s números racionais irredutíveis e maiores que zero. Então existe um número natural n_0 tal que $r < n_0 s$.*

Observação 3.4. A ideia da propriedade Arquimediana no conjunto dos números racionais é geometricamente interpretada em forma bem intuitiva como segue.
Imagine dois segmentos quaisquer de medida r e s, respectivamente, como na figura 3.2. Aqui estamos supondo $s < r$ pois se $r < s$ bastaria multiplicar s por $n_0 = 1$ para obter a afirmação.
Tomando agora sobre o segmento de medida r a partir de uma extremo, segmentos iguais de medida s, em certo momento superamos a medida de r, como mostra a figura 3.3.

Demonstração: Sejam $r = \frac{a}{b}$ e $s = \frac{c}{d}$ irredutíveis. Queremos provar que existe n_0 tal que

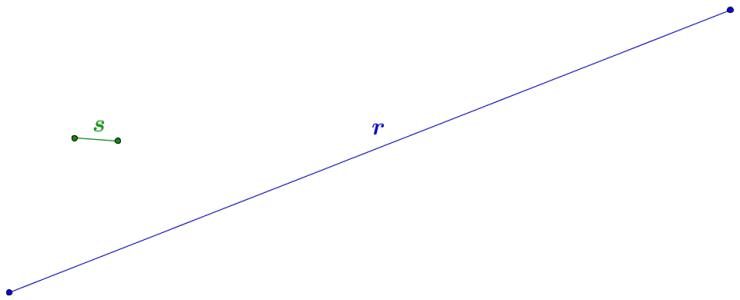


FIGURA 3.2: Os segmentos de medida r e s.

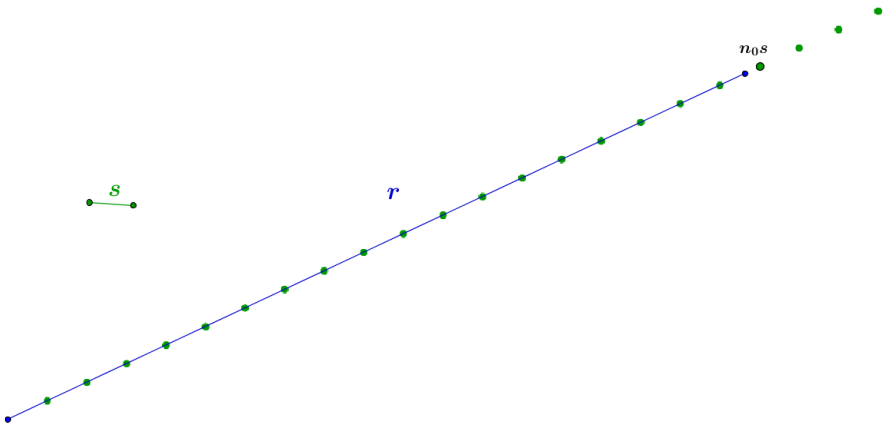


FIGURA 3.3: Os segmentos de medida s colocados um seguido de outro no segmento de medida r. O valor n_0 é mostrado exatamente quando supera o comprimento do segmento de medida r.

$r < n_0 s$, o que é equivalente a provar que

$$\frac{a}{b} < n_0 \frac{c}{d} \quad \text{que significa} \quad \frac{a}{b} < \overbrace{\frac{c}{d} + \frac{c}{d} + \ldots + \frac{c}{d}}^{n_0 \text{ parcelas}}. \tag{3.15}$$

Como temos

$$\overbrace{\frac{c}{d} + \frac{c}{d} + \ldots + \frac{c}{d}}^{n_0 \text{ parcelas}} = \frac{n_0 \cdot c}{d},$$

então, pela definição (3.12) e usando (3.15), obtemos

$$ad < n_0 cb. \tag{3.16}$$

Vamos efetuar a divisão inteira de ad por cb, obtendo o quociente q e resto r tais que

$$ad = qbc + r \text{ com } 0 \leq r < bc. \tag{3.17}$$

Somando bc a ambos os membros da igualdade em (3.17), obtém-se

$$ad + bc = qbc + bc + r \text{ ou equivalentemente } bc - r = (q+1)bc - ad,$$

de onde, usando agora a desigualdade $r < bc$ de (3.17), concluímos que

$$0 < (q+1)bc - ad,$$

que, comparada com (3.16), a desigualdade que queríamos chegar, nos mostra que podemos tomar $n_0 = q + 1$. ■

Note que a demonstração da propriedade 3.4 nos indica analiticamente como encontrar o n_0 da construção geométrica da figura 3.3. Vejamos um exemplo.

Exemplo 3.2. *Sejam os números racionais positivos* $\frac{3}{100}$ *e* $\frac{70}{3}$. *Vamos encontrar* n_0 *natural tal que* $n_0 \cdot \frac{3}{100} > \frac{70}{3}$.
Efetuamos os produtos "cruzados", $100 \cdot 70 = 7.000$ *e* $3 \cdot 3 = 9$, *achando a seguir o quociente da divisão inteira de* 7.000 *por* 9*:*

$$7.000 = 777 \cdot 9 + 7,$$

de onde, pela construção feita na proposição 3.4, temos que $n_0 = q + 1 = 777 + 1 = 778$. *Note que, de fato,*

$$778 \cdot \tfrac{3}{100} = \tfrac{2.334}{100}, \quad \textit{que é maior que} \quad \tfrac{70}{3} \quad \textit{pois}$$

$$7.002 = 2.334 \cdot 3 > 70 \cdot 100 = 7.000.$$

Também note que o $n_0 = 778$ *encontrado é o menor natural a verificar essa propriedade.*

Desafio!

Ache os naturais da propriedade arquimedeana dos pares de números racionais $(\frac{1}{789}, \frac{1002}{9})$ e $(\frac{7}{6}, \frac{673}{2})$. Anote-os no caderno

Clique aqui para ver a resposta.

A próxima proposição está relacionada com a **Densidade do Números Racionais**.

Proposição 3.5. *Dados dois números racionais r e s verificando $r < s$, então existe um número racional t tal que $r < t < s$. Ou seja, "entre" dois números racionais quaisquer existe um outro número racional.*

Demonstração: Seja $t = \frac{1}{2} \cdot (r + s)$. Então, pela monotonia da relação de ordem em $\mathbb{Q}$ (veja 3.1 item 2.1, pg. 138), temos que

$$\begin{aligned} r &= \tfrac{1}{2} \cdot r + \tfrac{1}{2} \cdot r \\ &< \tfrac{1}{2} \cdot r + \tfrac{1}{2} \cdot s \qquad \text{(que é o número } t\text{)} \\ &< \tfrac{1}{2} \cdot s + \tfrac{1}{2} \cdot s \\ &= s, \end{aligned}$$

como queríamos demonstrar. ■

3.2 Números Racionais Decimais

Representamos os números racionais como classes de equivalência de pares ordenados de números inteiros.

Existe uma outra forma de expressar um número racional, chamada de representação decimal.

Sabemos que os números inteiros podem ser representados com os dígitos de 0 a 9. Por exemplo, o número 30.459 é expresso como potências de 10, da forma:

$$30459 = 3 \cdot 10^4 + 0 \cdot 10^3 + 4 \cdot 10^2 + 5 \cdot 10^1 + 9 \cdot 10^0.$$

Da mesma forma poderíamos expressar o número racional por potências de 10 com expoente positivo ou negativo. Vejamos um exemplo.

Exemplo 3.3. A expressão decimal $3,58$ pode ser expressa como um número racional da forma $\frac{p}{q}$. De fato, usando potências de 10 obtemos que

$$\begin{aligned} 3,58 &= 3 \cdot 10^0 + 5 \cdot 10^{-1} + 8 \cdot 10^{-2} \\ &= 3 + \frac{5}{10} + \frac{8}{100} \\ &= \frac{300 + 50 + 8}{100} \\ &= \frac{358}{100}, \end{aligned}$$

o que mostra o afirmado.

A questão a ser resolvida seria a recíproca do exemplo 3.3, ou seja, qual seria a expressão que associaríamos a um número racional dado por $\frac{a}{b}$? Lembre que a e b são números inteiros e $b > 0$, portanto (veja módulo I, seção 1.6) existem q e r, quociente e resto da divisão inteira de a por b, tais que

$$a = b \cdot q + r, \text{ com } 0 < r < |b| = b. \tag{3.18}$$

Assim, podemos escrever o número racional $\frac{a}{b}$ a partir de (3.18) como

$$\begin{aligned} \frac{a}{b} &= \frac{b \cdot q + r}{b} \\ &= \frac{b \cdot q}{b} + \frac{r}{b} \\ &= q + \frac{r}{b}. \end{aligned}$$

Note que de (3.18) temos que $r < b$, de onde concluímos que o número racional $\frac{r}{b}$ é menor que 1. Assim, observamos que todo número racional pode ser escrito da forma:

$$\frac{a}{b} = q + \frac{r}{b}, \quad \text{com} \quad 0 < \frac{r}{b} < 1. \tag{3.19}$$

Como poderíamos expressar um número racional positivo e menor do que um por uma representação decimal?
Imaginamos que você ensina isso e está bem claro sobre como obtê-la. Correto?

Vamos analisar como é que faríamos esta transformação de um número racional para sua representação decimal em forma de algoritmo. Siga o exemplo seguinte.

Vimos que a representação como número racional do decimal $3,58$ é $\frac{358}{100}$. Fazendo a divisão inteira de 358 por 100, obtemos

$$358 = 3 \cdot 100 + 58 \text{ com } \frac{58}{100} < 1,$$

de onde gostaríamos expressar $\frac{58}{100}$ na forma

$$0, x_1 x_2 \ldots x_n \quad \text{para } n \text{ número natural}$$

ou, equivalentemente,

$$\frac{58}{100} = x_1 \cdot 10^{-1} + x_2 \cdot 10^{-2} + \ldots + x_n \cdot 10^{-n}. \tag{3.20}$$

Multipliquemos ambos os membros de (3.20) por 10, para obter

$$\frac{58}{10} = x_1 + x_2 \cdot 10^{-1} + \ldots + x_n \cdot 10^{-n+1}. \tag{3.21}$$

Dividindo novamente em forma inteira 58 por 10 temos como resultado

$$58 = 5 \cdot 10 + 8,$$

e usando (3.19), chegamos à expressão

$$\frac{58}{10} = 5 + \frac{8}{10}.$$

De esta última igualdade e (3.21), obtemos

$$5 + \frac{8}{10} = x_1 + x_2 \cdot 10^{-1} + \ldots + x_n \cdot 10^{-n+1} \tag{3.22}$$

Multipliquemos ambos os membros de (3.22) por 10 para obter

$$50 + 8 = 10x_1 + x_2 + \ldots + x_n \cdot 10^{-n+2}.$$

De esta última expressão, podemos concluir que

$$10x_1 = 50 \text{ e } x_2 = 8, \text{ ou seja, } x_1 = 5,\ x_2 = 8 \text{ e } x_i = 0 \text{ para } i = 3, \ldots, n. \tag{3.23}$$

Assim, de (3.20) e (3.23) obtemos que a expressão decimal de $\frac{58}{10}$ é $0,58$.

Imaginamos que você parou para pensar neste momento que a conclusão (3.18) é um fato bem conhecido desde a escola! Correto?
O que é para ser notado é que, na realidade, no exemplo foi descrito um *algoritmo* que dá surgimento à expressão decimal dos números racionais da forma $\frac{a}{b}$. Este algoritmo é descrito a seguir.

Algoritmo para obtenção da Expressão Decimal de $\frac{a}{b}$. (3.24)

Sem perda de generalidade, iremos supor $a > 0$.

1. Caso $\frac{a}{b} \geq 1$, calcule o quociente (q) e o resto (r) da divisão inteira de a por b.

   Caso contrário, escreva $\frac{a}{b} = 0, x_1.$, renomeie a como sendo r e passe ao item 3.

2. Caso que $r = 0$, o algoritmo para e a resposta é $\frac{a}{b} = q$.

   Caso contrário, escreva $\frac{a}{b} = q, x_1$, onde x_1 será determinado no próximo passo.

3. Calcule o quociente q_1 e resto r_1 da divisão inteira de $10r$ por b.

4. Caso que $r_1 = 0$, o algoritmo para e a reposta é $\frac{a}{b} = q, q_1$.

   Caso contrario, repita o item 3 renomeando $q_1 = q$ e $r_1 = r$.

Seguindo os comandos do algoritmo (3.24), vejamos como podemos expressar $\frac{9}{8}$ em forma decimal:

1. Calculamos o quociente e resto da divisão inteira de 9 por 8:

$$9 = 1 \cdot 8 + 1, \tag{3.25}$$

   de onde temos $q = 1$ e $r = 1$. Assim, como $r \neq 0$ escrevemos

$$\frac{9}{8} = 1, x_1.$$

2. Calculamos o quociente da divisão inteira $10 \cdot r = 10 \cdot 1 = 10$ por $b = 8$, que resulta em:

$$10 = 1 \cdot 8 + 2,$$

   e como o resto não é zero, escrevemos

$$\frac{9}{8} = 1, 1x_2.$$

3. Repetimos o passo 3, calculando o resto da divisão de $10 \cdot r_1 = 10 \cdot 2 = 20$ por $b = 8$, obtendo

$$20 = 2 \cdot 8 + 4,$$

   de onde, como o resto não é zero, escrevemos

$$\frac{9}{8} = 1, 12x_3.$$

Voltando ao item 3, da divisão inteira de $10 \cdot 4$ por $b = 8$, obtemos

$$40 = 5 \cdot 8 + 0,$$

parando asim o algoritmo.

Usando (3.25), temos como resposta final

$$\begin{aligned} \frac{9}{8} &= 1 + \tfrac{1}{8} \\ &= 1,125, \end{aligned}$$

ou, equivalentemente,

$$\frac{9}{8} = 1 \cdot 10^0 + 1 \cdot 10^{-1} + 2 \cdot 10^{-2} + 5 \cdot 10^{-3}.$$

Vejamos outro exemplo.

Exemplo 3.4. Sigamos os passos do algoritmo (3.24) (pg. 145) para o número racional $\frac{1}{3}$. Como $\frac{1}{3}$ é um número positivo menor do que 1, passamos diretamente para o terceiro item do algoritmo. Multiplicamos $a = 1$ por 10 e efetuamos a divisão inteira de 10 por 3:

$$10 = 3 \cdot 3 + 1, \tag{3.26}$$

escrevendo

$$\frac{1}{3} = 0,3x_2,$$

com x_2 a ser determinado no próximo passo do algoritmo, que consiste em multiplicar o resto da divisão inteira em (3.26) por 10 e dividir novamente por $b = 3$. Obtemos novamente (3.26), de onde temos que

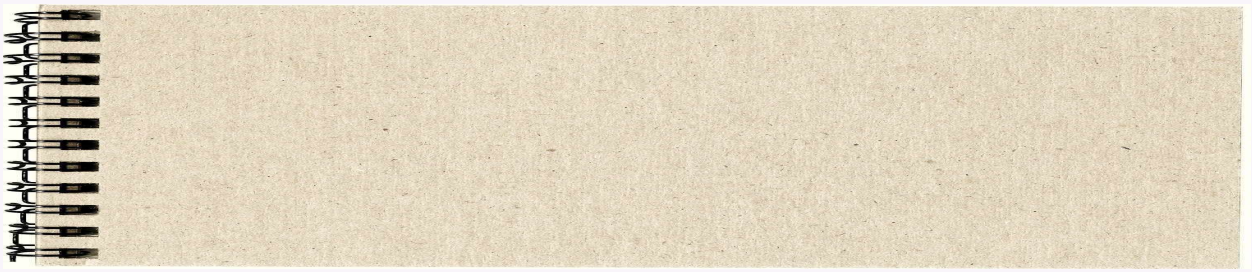
$$\frac{1}{3} = 0,33x_3,$$

sendo que o algoritmo não para porque sempre voltamos para a expressão (3.26) e portanto o resto nunca é zero.

Agora é sua vez! no próximo desafio.

Desafio!

Repita os passos do algoritmo (3.24) (pg. 145) para achar a expressão decimal de $\frac{65}{33}$. Não faça como na escola! Anote os passos do algoritmo no caderno.



Clique aqui para ver a resposta.

A expressão da equação (3.23), do desafio anterior e do exemplo 3.4, mostraram que há pelo menos duas possibilidades para a representação decimal de um número racional $\frac{a}{b}$ com $b > 0$:

$$\frac{a}{b} = q, x_1x_2 \ldots x_n \quad \text{ou} \quad \frac{a}{b} = q, x_1x_2 \ldots,$$

isto é, pode ter um representação decimal finita ou uma expressão decimal infinita.

Por que é que alguns números racionais têm representação decimal finita e outros não? Qual é a propriedade comum aos números racionais com qualidade de terminar o algoritmo pg. 145 da representação decimal?

Note que, se um número racional r tem uma representação decimal finita, depois da vírgula só tem um número finito de dígitos. Portanto, se multiplicarmos r por uma potência de 10, digamos 10^s para um s conveniente, teríamos $10^s \cdot r$ um número inteiro. É o que diríamos na escola, "corremos" a vírgula tantas casas à direita como o número s. Por exemplo, o número $r = 36,125$, que tem um representação decimal finita, multiplicado por 10^3, se transforma no número inteiro $n = 36.125$.

Observe também que a fração $\frac{36.125}{1.000}$ é igual a $\frac{17^2 \cdot 5^3}{2^3 \cdot 5^3} = \frac{17^2}{2^3}$. O denominador da fração irredutível é uma potência de 2.

Outro exemplo mais simples é da expressão decimal $1,2$ do número racional $\frac{12}{10} = \frac{3 \cdot 2^2}{2 \cdot 5}$, cuja fração irredutível é $\frac{3 \cdot 2}{5}$ e que possui no seu denominador o número 5.

Reciprocamente, se temos um número racional do tipo $r = \frac{1}{2^3 \cdot 5^2}$, então $10^3 \cdot r = 5$. Portanto, $r = \frac{5}{10^3}$, que é a representação decimal de r. Veja que essa representação é finita!

A seguinte proposição formaliza as ideias analisadas.

Proposição 3.6. *Um número racional cujo representante é irredutível tem expressão decimal finita se e somente se o denominador possui uma fatorização prima constituída por somente por potências de* 2 *e* 5*.*

Demonstração: Suponha que $\frac{a}{b}$ tem uma representação finita dada por

$$\frac{a}{b} = q \cdot 10^0 + x_1 \cdot 10^{-1} + x_2 \cdot 10^{-2} \ldots x_n \cdot 10^{-n}. \tag{3.27}$$

Multiplicando ambos os membros de (3.27) por 10^n, obtemos

$$10^n \cdot \tfrac{a}{b} = q \cdot 10^n + x_1 \cdot 10^{n-1} + x_2 \cdot 10^{n-2} \ldots x_n \cdot 10^0 = n_0,$$

onde n_0 é um número inteiro. Assim, podemos escrever

$$\frac{a}{b} = \frac{n_0}{10^n},$$

o que mostra que a fração $\frac{a}{b}$ é equivalente a uma fração com denominador com uma fatorização apenas formada com fatores 2 e 5.

Reciprocamente, suponha que o número racional r tem como representante irredutível a fração

$$r = \frac{n_0}{2^s 5^t}, \tag{3.28}$$

com s e t números naturais. Vamos provar que a representação decimal de r é finita. Suponha $s > t$, pois, caso sejam iguais, tomamos para nosso raciocínio $t = s$ e, no caso que $t > s$, renomeamos $s = t$ e $t = s$. Com estas convenções, multipliquemos ambos os membros de (3.28) por 10^s. Obtemos que

$$10^s \cdot r = n_1,$$

onde n_1 é um número inteiro positivo que tem uma expressão decimal finita

$$n_1 = x_1 \cdot 10^0 + x_2 \cdot 10^1 \ldots x_m \cdot 10^m, \tag{3.29}$$

com $m \leq s$. Assim, dividindo (3.29) ambos os membros por 10^s obtemos

$$r = x_m \cdot 10^{m-s} + x_{m-1} \cdot 10^{(m-1)-s} \ldots x_1 \cdot 10^{-s},$$

o que mostra que a expressão decimal de r é finita.

■

Para esclarecer melhor a proposição 3.6 vamos ilustrar a ideia com um exemplo.

Exemplo 3.5. Seja o número racional $r = \frac{3}{2^3 5^7}$. Claramente é irredutível pois $\text{MDC}(3, 2^3 5^7) = 1$. Vamos mostrar que r tem representação decimal finita de acordo com a proposição 3.6. Na demonstração, é usado o maior dos dois expoentes dos fatores 2 e 5 que, neste caso, é 7. Multiplicamos r por 10^7 obtendo a partir daí que

$$\begin{aligned} 10^7 \cdot r &= 10^7 \cdot \frac{3}{2^3 5^7} \\ &= 2^3 \cdot 2^4 \cdot 5^7 \frac{3}{2^3 5^7} \\ &= 2^4 \cdot 3 \\ &= 48 \\ &= 8 \cdot 10^0 + 4 \cdot 10^1, \end{aligned}$$

de onde obtemos que

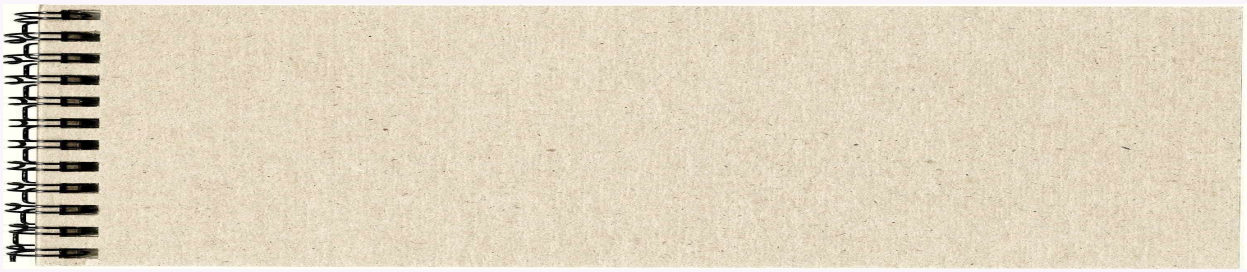
$$\begin{aligned} r &= \frac{8 \cdot 10^0 + 4 \cdot 10^1}{10^7} \\ &= 4 \cdot 10^{-6} + 8 \cdot 10^{-7}, \end{aligned}$$

que é a representação decimal finita de r.

A seguir mais um desafio para praticar as ideias do exemplo 3.5.

Desafio!

Pela fatoração prima dos seus denominadores, determine se os números racionais $\frac{101}{99}$ e $\frac{19.283}{6.250}$ tem representação finita. No caso afirmativo calcule dsua representação decimal.



Clique aqui para ver a resposta.

O que têm em comum os números $43,65;\ 43,98;\ 43,999$ ou os números $-43,65;\ -43,98;\ -43,999$?.

E que têm em comum ambos os grupos de números?

O que têm em comum $43,65;\ 43,98;\ 43,999$ é o inteiro 43 e que todos eles são maiores que este número. Da mesma forma temos que $-43,65;\ -43,98;\ -43,999$ têm em comum o número inteiro -43, que é maior que todos. Essa caraterística é espressa na seguinte definição.

Definição 3.6. *Seja x um número racional. Definimos*

$$\lfloor x \rfloor = \textit{o maior inteiro menor ou igual a } x$$

$$\lceil x \rceil = \textit{o menor inteiro maior ou igual a } x$$

$\lfloor x \rfloor$ *é a* **parte inteira por excesso** *de x e $\lceil x \rceil$ é a* **parte inteira por defeito** *de x.*

Exemplo 3.6. Veja que temos $\lfloor 3,1 \rfloor = 3$, $\lceil 3,1 \rceil = 4$, $\lfloor -3,1 \rfloor = -4$ e $\lceil -3,1 \rceil = -3$
Também da definição concluímos que $\lfloor 3 \rfloor = 3$ e $\lceil 3 \rceil = 3$.

Observação 3.5. A mesma definição pode ser usada para os números reais, em geral como veremos no módulo 4. À parte inteira de um número real podemos associar a função teto e a função piso ilustradas na figura 3.4

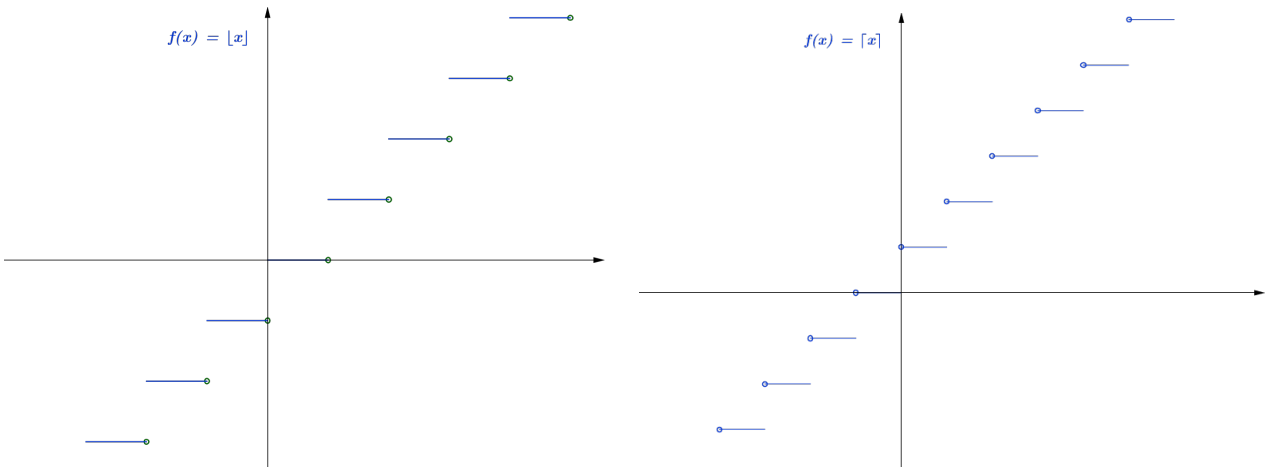


FIGURA 3.4: A função piso $f(x) = \lfloor x \rfloor$ e a função teto $f(x) = \lceil x \rceil$.

Resumindo as propriedades da parte inteira de um número real, obtemos o quadro 3.2 seguinte:

Propriedades 3.2.

$$\lfloor x \rfloor = \max\{n \in \mathbb{Z} \mid n \leq x\} \tag{3.30}$$

$$n = \lfloor x \rfloor \text{ se e somente se } n \leq x < n+1. \tag{3.31}$$

$$\lfloor x \rfloor \leq x \text{ para todo } x \tag{3.32}$$

$$\lfloor x \rfloor = x \iff x \in \mathbb{Z}. \tag{3.33}$$

O seguinte lema é consequência das propriedades enunciadas em 3.2.

Lema 3.1. *Para todo* $x \in \mathbb{R}$

$$x - 1 < \lfloor x \rfloor \leq x.$$

Demonstração: Pela propriedade (3.31), temos que $n \leq x < n+1$. Portanto, $x - 1 < n$ e pela propriedade (3.32), obtemos que $x - 1 < \lfloor x \rfloor$. ■

Sabemos que há números racionais com uma caraterística que os distingue, que é a periodicidade da sua **dízima** 

.
Você já se questionou qual é a razão pela qual os números racionais têm o que chamamos de expressão decimal periódica?.

Vejamos este fato em um exemplo para depois justificar teoricamente.

Exemplo 3.7. Vamos achar a expressão decimal do número racional $r = \frac{5}{7}$. Como indica pg. 145, do fato de que $\frac{5}{7} < 1$, multiplicamos o numerador 5 por 10 e com o resultado efetuamos a divisão inteira por 7, continuando o processo sucessivo do algoritmo para obter

$$\begin{aligned} 50 &= 7 \cdot 7 + 1 \\ 10 &= 1 \cdot 7 + 3 \\ 30 &= 4 \cdot 7 + 2 \\ 20 &= 2 \cdot 7 + 6 \\ 60 &= 8 \cdot 7 + 4 \\ 40 &= 5 \cdot 7 + 5, \end{aligned}$$

neste momento voltamos ao primeiro cálculo e portanto a *periodicidade* da expressão decimal de r, que é $0,714285$. Observe que os restos da divisão por 7 só podem ser elementos do conjunto $\{0,\ 1, 2, 3,\ 4, 5,\ 6\}$, que é um conjunto *finito*!.

Generalizamos a ilustração do exemplo 3.7 na seguinte proposição.

Proposição 3.7. *Seja r um número racional representado por uma fração irredutível $\frac{a}{b}$ com $b > 0$. Supondo que a expressão decimal de r não é finita, então esta expressão tem a forma*

$$q_1, q_2 q_3 \ldots q_m \overline{q_{m+1} q_{m+2} \ldots q_n}, \tag{3.34}$$

com $m,\ n$ naturais e $\overline{q_{m+1} q_{m+2} \ldots q_n}$ representa a sequência de números

$$\{q_{m+1},\ q_{m+2}, \ldots, q_n,\ q_{m+1},\ q_{m+2}, \ldots, q_n, \ldots\}. \tag{3.35}$$

Demonstração: Como r é representado por uma fração irredutível, o algoritmo para calcular a expressão decimal de r começa dividindo a por b. Seja r_1 o resto desta divisão inteira. Temos pelo algoritmo da divisão inteira (veja módulo 1, 1.6, pg.56) e do fato que r tem uma representação decimal não finita que

$$0 < r_1 \leq b - 1. \tag{3.36}$$

Multiplicamos r_1 por 10 e seguindo o algoritmo 3.24 o dividimos por b. Continuando o algoritmo, obtemos uma sequência de restos $\{r_1,\ r_2,\ r_3, \ldots\}$ em que cada um dos elementos da sequência verifica (3.36). Assim a sequência de restos só podem ser números entre 0 e $b - 1$, ou seja, só pode ser uma sequência finita. Isso mostra na expressão (3.35) que $m,\ n$ são naturais dados.

A razão pela qual a sequência dos quocientes do algoritmo pg. 145 tem repetição *ordenada* como descrito em (3.35) provém do fato de que se existir $r_i = r_j$ para algum i, j então devemos ter $10 \cdot r_i = 10 \cdot r_j$ e assim o resto e quociente da divisão desses números por b coincidem.

Isto significa que $q_{i+1} = q_{j+1}$, o que mostra que a sequência inicial dos quocientes se repete a partir de uma igualdade de restos. ■

Definição 3.7. *Diz-se que o número racional r é periódico se sua representação decimal não é finita, ou seja é da forma* (3.34).
Definimos o número racional r como periódico puro se sua representação decimal é da forma

$$r = q_1, \overline{q_2, q_3, \ldots q_n}, \tag{3.37}$$

Observação 3.6. Os números racionais periódicos que não são puros são a soma de um número racional de representação *finita* com um periódico puro.
Por exemplo, o número racional $4, 36\overline{789}$ é a soma de $4, 36$, número racional de representação decimal finita com $0, 00\overline{789}$ que é um número racional periódico puro.

A questão agora é como achar o representante irredutível de um número racional r do qual conhecemos a representação decimal periódica. Vejamos isto com um exemplo.

Exemplo 3.8. Suponha que conhecemos a representação decimal do número racional r dada por $4, 36\overline{789}$. Queremos saber um representante desse número racional por uma fração irredutível.
Da observação 3.6 temos que $r = 4, 36 + 0, 00\overline{789}$. Assim podemos escrever a expressão decimal de $4, 36$ como $4 + \frac{3}{10} + \frac{6}{100}$. Falta saber qual é a representação decimal de $0, 00\overline{789}$, já que, somando ambas expressões, teríamos a representação decimal de r.

Vamos então revisar como é a obtenção da expressão decimal do número racional de representante irredutível periódico puro. Continuemos nosso exemplo.

A ideia é associar ao número racional periódico puro $0, \overline{789}$ a fração cujo denominador é o período e o numerador é o número $\overline{99\ldots9}$, ou seja, um número que contenha tantos dígitos noves quanto o comprimento do período do número racional. Neste caso é a fração $\frac{789}{999}$.

Vejamos que esta associação é conveniente fazendo o processo inverso: passando da fração irredutível $\frac{789}{999}$ para a expressão decimal $0, \overline{789}$, como mostrado a seguir.

$$\begin{aligned} 7890 &= 7 \cdot 999 + 897 \\ 8970 &= 8 \cdot 999 + 978 \\ 9780 &= 9 \cdot 999 + 789, \end{aligned} \tag{3.38}$$

voltando neste momento para a primeira divisão, o que mostra que

$$\frac{789}{999} = 0,\overline{789}.$$

Assim o número racional $4,36\overline{789}$ pode ser escrito como

$$4 + \frac{36}{100} + \frac{789}{99900} = \frac{436353}{99900}.$$

Observação 3.7. Note que, nas divisões da equação (3.38), quando o número $10 \cdot 789$ é dividido por 999, o resto obtido é 897. Isto está relacionado com multiplicar por 10 o número $0,789789789\ldots$, que dá como resultado $7,\ 897\ 89789\ldots$.
Da mesma maneira, o resultado de multiplicar por 10 o número $7,89789789\ldots$ é $78,\ 978\ 9789\ldots$, onde os dígitos remarcados formam um número que é exatamente o resto da segunda divisão inteira em (3.38).

Vamos formalizar a ideia da observação 3.7 na seguinte proposição.

Proposição 3.8. *Seja a um número inteiro positivo de n dígitos tal que $a \neq 10^n - 1$. Então, a divisão inteira de $10 \cdot a$ pelo número $b = \underbrace{99\ldots9}_{n \text{ noves}}$ dá como resultado o primeiro dígito de a e como resto o número obtido com os restantes dígitos de a.*

Demonstração: Suponha que $a = a_1 + a_2 \cdot 10$, ou seja, é um número inteiro com dois dígitos. Pela condição que $a \neq 10^n - 1$, devemos ter $0 \leq a_1 \leq 9$ e $1 \leq a_2 < 9$, de onde

$$10 \cdot a_1 + a_2 < 99. \tag{3.39}$$

Por outro lado temos que

$$\begin{aligned} 10 \cdot a &= a_1 \cdot 10 + a_2 \cdot 10^2 \\ &= a_1 \cdot 10 + a_2 \cdot (99 + 1) \\ &= a_2 \cdot 99 + a_1 \cdot 10 + a_2, \end{aligned}$$

que junto com (3.39) e pela unicidade do quociente e resto (veja no módulo II, teorema 1.2, pg.57) da divisão inteira de $10 \cdot a$ por 99 que a_2 e $a_1 \cdot 10 + a_2$ são quociente e resto, respectivamente, dessa divisão.

Com um argumento por indução podemos provar a proposição da mesma maneira para um número a de n dígitos. ■

Corolário 3.1. *Suponha que a fração irredutível $\frac{a}{b}$ tem um período de comprimento l. Então $b \mid 10^l - 1$.*

Demonstração: De fato, como a fração representa um número racional de período puro com l dígitos, então o numerador é o número inteiro positivo c, formado por esses dígitos.

Por outro lado, o denominador é o número inteiro positivo formado por l noves que pode ser escrito como $10^l - 1$. Isto significa que $\frac{a}{b} = \frac{c}{10^l - 1}$, de onde $10^l - 1$ é um múltiplo de b, como foi afirmado. ■

Observação 3.8. Algumas observações importantes:

1. Com a proposição 3.8 temos completado a prova de que existe uma bijeção entre números racionais e expressões decimais periódicas cujo período seja diferente de $\overline{99\ldots9}$.
2. Em particular, podemos saber o período de uma fração irredutível $\frac{a}{b}$ calculando a mínima potência de 10 que é congruente com 1 no módulo b.

Vamos ilustrar os itens 1 e 2 da observação 3.8 com um exemplo.

Exemplo 3.9. Vamos analisar o número racional $r = \frac{1}{7}$ usando o item 2 da observação 3.8. Temos que

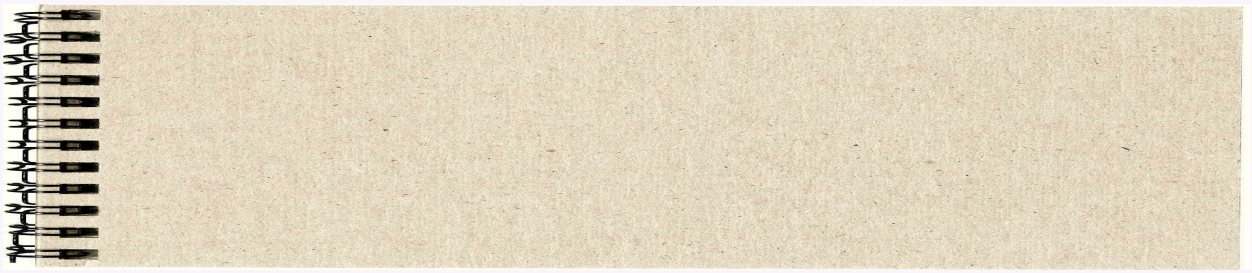
$$\begin{aligned} 10^1 &\equiv 3 \pmod 7 \\ 10^2 &\equiv 2 \pmod 7 \\ 10^3 &\equiv 6 \pmod 7 \\ 10^4 &\equiv 4 \pmod 7 \\ 10^5 &\equiv 5 \pmod 7 \\ 10^6 &\equiv 1 \pmod 7 \end{aligned}$$

portanto $7 \mid 10^6 - 1$ é a menor potência de 10 com essa propriedade.

Assim, usando o item 2 da observação 3.8, temos que o período de r tem comprimento 6.

Desafio!

Calcular o comprimento do período da representação decimal de $r = 1/3663$, sem calcular explicitamente o período.



Clique aqui para ver a resposta.

3.3 A Noção de Enumeração no Conjunto dos Números Racionais

Usando a proposição 3.5, temos que entre 0 e 1 encontramos o número racional $\frac{0+1}{2} = \frac{1}{2}$. Aplicando novamente a proposição obtemos entre 0 e $\frac{1}{2}$ o número racional $\frac{0+\frac{1}{2}}{2} = \frac{1}{4}$. Logo, usando repetidamente n vezes a proposição, podemos conseguir o conjunto

$$0,\ \tfrac{1}{2^n},\ \tfrac{2}{2^n}, \ldots, \tfrac{2^n}{2^n} = 1$$

que quando n é grande nos dá um número também grande de números racionais bem próximos, a uma distância $\frac{1}{2^n}$

Observando estes números racionais na reta geométrica, como mostrado na figura 3.5, notamos que há "muito" mais números racionais que números naturais, pois podemos estender o processo feito no intervalo $[0, 1]$ a qualquer intervalo $[n, n+1]$

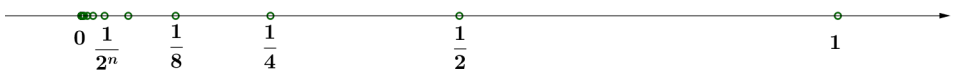


FIGURA 3.5: A reta racional entre 0 e 1.

Porém, nesta seção veremos que os números racionais, se "contados", existem tanto quanto números naturais. Isto será formalizado com o conceito de enumeração, que está associado a outro conceito matemático importante, que é a cardinalidade de um conjunto. Começaremos esta seção com esta definição.

Definição 3.8. *Diz-se que o conjunto A é finito se tem a mesma cardinalidade do conjunto $\{1, 2, 3, \ldots, n\}$ para algum $n \in \mathbb{N}$ ou $A = \emptyset$.*
Diz-se que o conjunto A é infinito se A não é finito.

Exemplo 3.10. O conjunto $A = \{-1, -2, -3, -4\}$ tem cardinalidade 4, pois existe a função $f : I_4 = \{1, 2, 3, 4\} \to A$ definida por $f(x) = -x$, que é uma função bijetora. A função f está ilustrada na Figura 3.6.

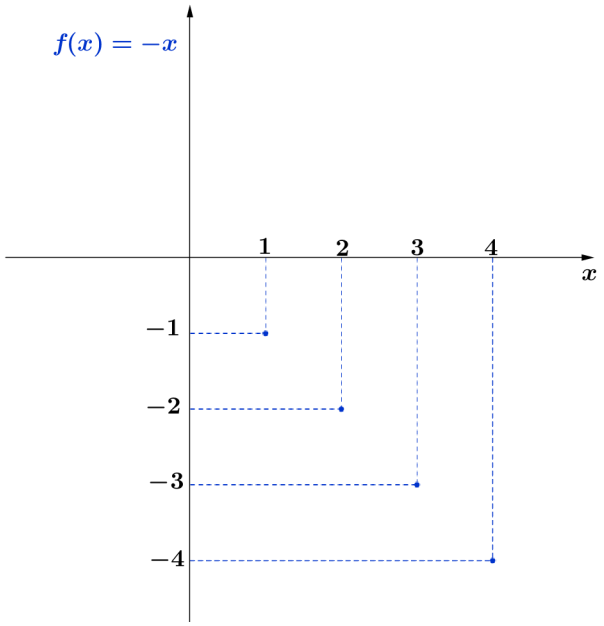


FIGURA 3.6: A bijeção f entre I_4 e o conjunto A.

Definição 3.9. *Um conjunto X se diz infinito se não for finito; X se diz enumerável se for finito ou se existir uma bijeção $f : \mathbb{N} \to X$.*
Diz-se que X tem a mesma cardinalidade que $\mathbb{N}$.

A cardinalidade do conjunto dos naturais é denotada por $\aleph_0$, onde aleph é o símbolo da figura 3.7.

FIGURA 3.7: A letra do alfabeto hebreu.

Exemplo 3.11. O conjunto dos números naturais pares, $P = \{m = 2k,\ k \in \mathbb{N}\}$ tem a mesma cardinalidade que $\mathbb{N}$. De fato, basta estabelecer a bijeção $f : \mathbb{N} \to P$ definida por $f(n) = 2n$, como mostra a Figura 3.8

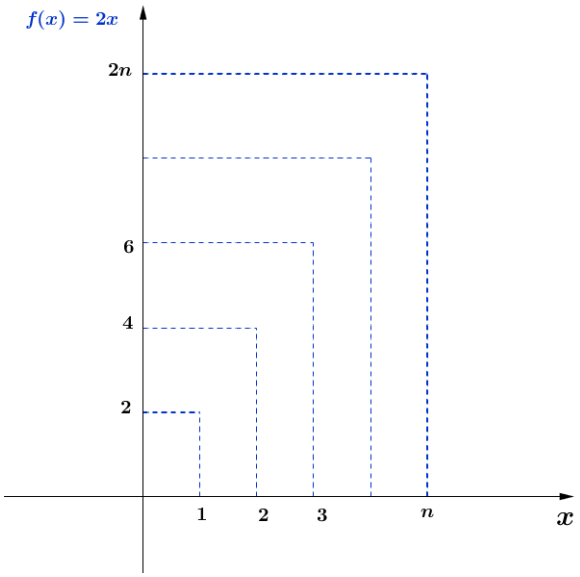
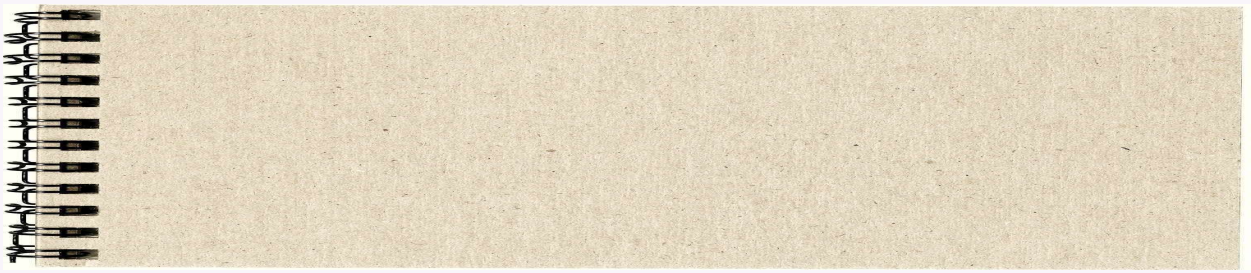


FIGURA 3.8: A bijeção f entre $\mathbb{N}$ e o conjunto P.

Desafio!

Mostre que o conjunto dos números inteiros ímpares é enumerável. Anote a prova no caderno.



Clique aqui para ver a resposta.

Exemplo 3.12. Com a função $f(x) = -x$ podemos estabelecer uma bijeção entre o conjunto dos números naturais, $\mathbb{N}$, e o conjunto dos números inteiros negativos, $\mathbb{Z}^-$, mostrando com isto que $\mathbb{Z}^-$ é um conjunto enumerável. Esta bijeção está ilustrada na Figura 3.9.

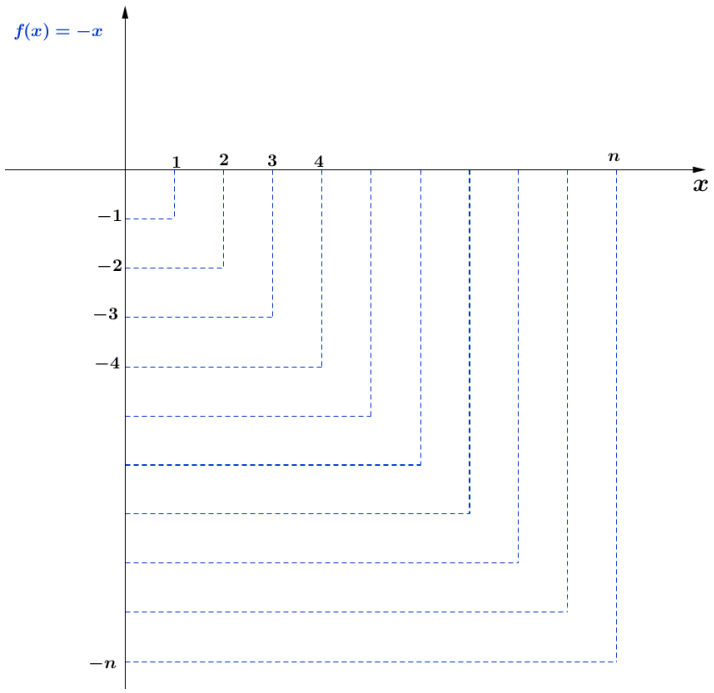
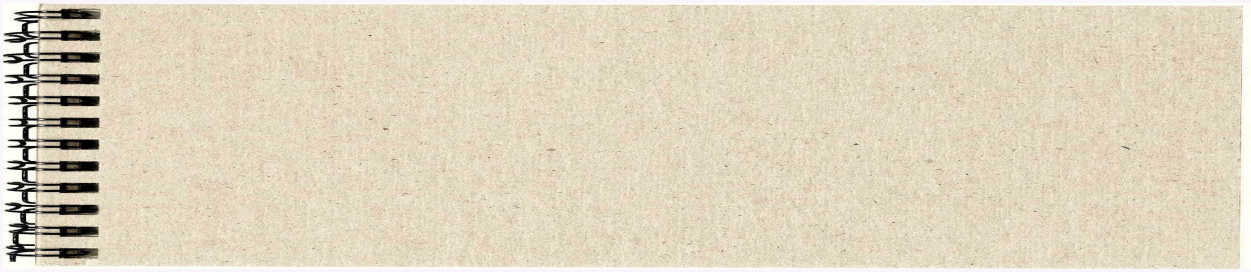


FIGURA 3.9: A bijeção f entre $\mathbb{N}$ e $\mathbb{Z}^-$.

Desafio!

Faça a tabela das 10 primeiras imagens pela função $f : \mathbb{N} \to \mathbb{Z}$ definida por $f(n) = (-1)^n \lfloor \frac{n}{2} \rfloor$. Note que f é um bijeção, mostrando que $\mathbb{Z}$ é enumerável e tem a mesma cardinalidade de $\mathbb{N}$.



Clique aqui para ver a resposta.

A seguir enunciamos e damos uma ideia da demonstração de que o conjunto $\mathbb{N} \times \mathbb{N}$ é infinito enumerável.

Proposição 3.9. *O conjunto $\mathbb{N} \times \mathbb{N}$ é infinito enumerável.*

Demonstração: Vamos estabelecer uma bijeção entre $\mathbb{N}$ e $\mathbb{N} \times \mathbb{N}$. Para construir este conjunto, tomemos primeiramente o elemento $x_1 = (1, 1)$. Note que não existe outro elemento em

$\mathbb{N} \times \mathbb{N}$ tal que a soma do primeiro elemento do par com o segundo elemento dê como resultado 2, ou seja, o par $(1, 1)$ é o único que verifica a propriedade $1 + 1 = 2$.

A seguir vamos procurar em $\mathbb{N} \times \mathbb{N}$ pares que verifiquem que a soma do primeiro elemento do par com o segundo elemento dê como resultado 3. Estes pares são

$$(1, 2) \text{ e } (2, 1) \text{ porque } 1 + 2 = 3 \text{ e } 2 + 1 = 3.$$

A seguir procuramos os pares de $\mathbb{N} \times \mathbb{N}$ tais que a soma é 4, que seriam $(1, 3)$, $(2, 2)$ e $(3, 1)$, e assim sucesivamente. Ordenando $\mathbb{N} \times \mathbb{N}$ da forma

$$\{(1, 1),\ (1, 2),\ (2, 1),\ (1, 3),\ (2, 2),\ (3, 1), \ldots\} \tag{3.40}$$

podemos estabelecer uma bijeção com $\mathbb{N}$, como mostra a tabela 3.1. Isto é uma uma ideia gráfica da prova. ■

$\mathbb{N} \to \mathbb{N} \times \mathbb{N}$
$1 \to (1, 1)$
$2 \to (1, 2)$
$3 \to (2, 1)$
$4 \to (1, 3)$
$5 \to (2, 2)$
$6 \to (3, 1)$
$7 \to (1, 4)$
$8 \to (2, 3)$
$9 \to (3, 2)$
$10 \to (4, 1)$
$11 \to (1, 5)$
$12 \to (2, 4)$
$13 \to (3, 3)$
$14 \to (4, 2)$
$15 \to (5, 1)$
$\ldots$

TABELA 3.1: A correspondência bijetora entre $\mathbb{N}$ e $\mathbb{N} \times \mathbb{N}$.

Na seguinte proposição, enunciamos e damos uma ideia da demonstração de que o conjunto números racionais é infinito enumerável

Proposição 3.10. *O conjunto dos números racionais é infinito enumerável.*

Demonstração: Podemos usar o mesmo procedimento usado na proposição 3.9 para mostrar que o conjunto dos números racionais positivos é infinito enumerável, ou seja, existe uma correspodência entre $\mathbb{N}$ e $\mathbb{Q}^+$.

Iniciamos, como na proposição 3.9, com o número racional $\frac{1}{1}$, que é o representante cujo numerador somado com denominador dá como resultado 2. Esse número racional é a imagem de 1. A imagem de 2 é o número racional representado por $\frac{1}{2}$ tal que a soma de numerador e denominador é 3. Podemos estabelecer uma bijeção de $\mathbb{N}$ em $\mathbb{Q}^+$, como mostra a tabela 3.2. ■

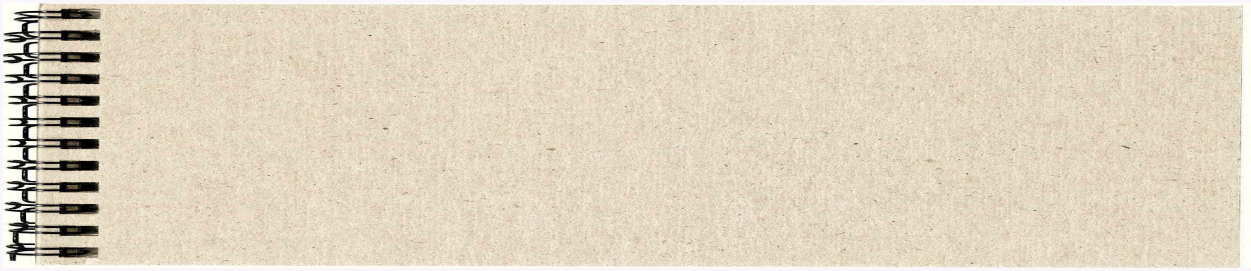
$\mathbb{N} \to Q^+$
$1 \to \frac{1}{1}$
$2 \to \frac{1}{2}$
$3 \to \frac{2}{1}$
$4 \to \frac{1}{3}$
$5 \to \frac{3}{1}$
$6 \to \frac{1}{4}$
$7 \to \frac{2}{3}$
$8 \to \frac{3}{2}$
$9 \to \frac{4}{1}$
$10 \to \frac{1}{5}$
$11 \to \frac{5}{1}$
$\ldots$

TABELA 3.2: A função bijetora entre $\mathbb{N}$ e $\mathbb{Q}^+$. Note que há uma diferença com a bijeção da proposição 3.9, seguindo a regra (3.1), onde os pares $(2,2)$, $(3,3)$ ou $(2,1)$ e $(4,2)$ são considerados, pois são pares diferentes entre si. Mas no conjunto dos números racionais temos que $\frac{2}{2} = \frac{3}{3}$, portanto esses números não são considerados repetidos na função.

Finalizamos este módulo com um desafio!

Desafio!

Dado um número racional $\frac{p}{q} \neq 0$ irredutível e um natural positivo n, que condições devem verificar p, q e n para que exista um número racional r tal que $r^n = \frac{p}{q}$?



Clique aqui para ver a resposta.

3.4 Respostas aos desafios do módulo 3

- Desafio da página 130.

  Reflexiva: por definição, $(a, b) \sim (a, b)$ se $a \cdot b = b \cdot a$, o que é verdadeiro pois a multiplicação de números inteiros é comutativa.

  Simétrica: se $(a, b) \sim (c, d)$ é válido que $(c, d) \sim (a, b)$? Temos por definição que

  $$\begin{array}{lll} (a,b) \sim (c,d) & \text{se e somente se} & a \cdot d = b \cdot c \\ (c,d) \sim (a,b) & \text{se e somente se} & c \cdot b = d \cdot a, \end{array}$$

  que são proposições equivalentes pela comutativa da multiplicação de números inteiros.

  Transitiva: se $(a, b) \sim (c, d)$ então temos

  $$a \cdot d = b \cdot c.$$

  Também se $(c, d) \sim (e, f)$ sabemos que

  $$c \cdot f = d \cdot e.$$

  Multiplicando a primeira igualdade por f que não é nulo e a segunda por b, que também não é nulo, obtemos

  $$a \cdot d \cdot f = b \cdot c \cdot f \quad \text{e} \quad b \cdot c \cdot f = b \cdot d \cdot e,$$

  de onde concluímos que $a \cdot d \cdot f = b \cdot d \cdot e$. Assim, cancelando d, que é não nulo, obtemos $a \cdot f = b \cdot e$ que significa por definição que $(a, b) \sim (e, f)$.

- Desafio da página 135.

$[(-240, 12)] = [(-20, 1)]$;
$[(-890, -355)] = [(178, 71)]$;
$[(5.003, 1110)]$ é irredutível.

No caso de $[(-890, -355)]$, você pode usar a fatoração prima para obter $890 = 2 \cdot 5 \cdot 89$ e $355 = 5 \cdot 71$, onde 71 é primo, pois os possíveis divisores primos do maior natural menor que $\sqrt{71}$ são $2,\ 3,\ 5$ e 7, que não dividem a 71. Lembre da propriedade observada no módulo I (observação 1.17, 75).

Da mesma maneira podemos mostrar que 5.003 é primo. Este é mais um desafio para você!

- Desafio da página 135.

  Como temos $\frac{a}{b} = \frac{c}{d}$ então devemos ter

  $$a \cdot d = b \cdot c. \tag{3.41}$$

  Como a fração $\frac{a}{b}$ é irredutível, então $\mathrm{MDC}(a, b) = 1$. Assim, $b \mid d$ (por quê? você sabe explicar? procure as proposições que aqui foram usadas!)

  Assim existe m tal que $d = b \cdot m$. Substituindo na igualdade (3.41), obtemos que

  $$a \cdot b \cdot m = b \cdot c,$$

  de onde, cancelando b, que não é nulo, obtemos que $a \cdot m = c$, como queríamos provar.

- Desafio da página 141.

  Efetuamos os produtos cruzados $1 \cdot 9 = 9$ e $789 \cdot 1002 = 790.578$ e a seguir

  $$\begin{array}{r|l} 790578 & 9 \\ \hline 0 & 87842 \end{array}$$

  Portanto, o menor número natural (de Arquimedes) de forma que $n_0 \frac{1}{789} > \frac{1002}{9}$ é $n_0 = 87.843$.

  Os produtos cruzados de $\frac{7}{6}$ e $\frac{673}{2}$ são 14 e 4.038, que têm como quociente e resto da divisão inteira

  $$\begin{array}{r|l} 4038 & 14 \\ \hline 6 & 288 \end{array}.$$

  Portanto, o número arquimedeano de forma que $n_1 \cdot \frac{7}{6} > \frac{673}{2}$ é $n_1 = 289$.

- Desafio da página 147.

  Seguindo o algoritmo:

  1. Calculamos o quociente e resto da divisão inteira de 65 por33:

     $$\begin{array}{r|l} 65 & 33 \\ \hline 32 & 1 \end{array}\ , \tag{3.42}$$

de onde temos $q = 1$ e $r = 32$. Assim, como $r \neq 0$ escrevemos

$$\frac{65}{33} = 1, x_1.$$

2. Calculamos o quociente da divisão inteira de $10 \cdot 32 = 320$ por $b = 33$, que resulta em:

$$\begin{array}{r|l} 320 & 33 \\ \hline 23 & 9 \end{array}$$

e como o resto não é zero, escrevemos

$$\frac{65}{33} = 1, 9x_2.$$

3. Repetimos o passo 3, calculando o resto da divisão de $10 \cdot r_1 = 10 \cdot 23 = 230$ por $b = 33$, obtendo

$$\begin{array}{r|l} 230 & 33 \\ \hline 32 & 6 \end{array} \quad ,$$

de onde, como o resto não é zero, escrevemos

$$\frac{65}{33} = 1, 96x_3.$$

Voltando ao item 3, teríamos que fazer a divisão inteira de $10 \cdot 320$ por $b = 33$, que é a divisão do item 1. Assim, o algoritmo não para!

- Desafio da página 149.

Pela fatoração prima dos seus denominadores temos que $r_1 = \frac{101}{99}$ não tem fatores primos 2 e 5 pois $99 = 3^2 \cdot 11$, logo sua representação decimal não é finita.

O número racional $r_2 = \frac{19.283}{6.250}$ tem representação finita, pois $6.250 = 2 \cdot 5^5$, possuindo o denominador fatores primos 2 e 5. Efetuando a divisão inteira, obtemos

$$\begin{array}{r|l} 19283 & 6250 \\ \hline 533 & 3 \end{array} \quad \text{de onde} \quad \frac{19.283}{6.250} = 3, x_1.$$

Prosseguindo o algoritmo:

$$\begin{array}{r|l} 5330 & 6250 \\ \hline 5330 & 0 \end{array} \quad \rightarrow \quad \frac{19.283}{6.250} = 3, 0x_2.$$

$$\begin{array}{r|l} 53300 & 6250 \\ \hline 3300 & 8 \end{array} \quad \rightarrow \quad \frac{19283}{6250} = 3, 08x_3.$$

$$\begin{array}{r|l} 33000 & 6250 \\ \hline 1750 & 5 \end{array} \quad \rightarrow \quad \frac{19283}{6250} = 3, 085x_4.$$

$$\begin{array}{r|l} 17500 & 6250 \\ \hline 5000 & 2 \end{array} \quad \rightarrow \quad \frac{19283}{6250} = 3,08528x_5.$$

$$\begin{array}{r|l} 50000 & 6250 \\ \hline 0 & 8 \end{array},$$

parando o algoritmo porque o resto é zero. Assim,

$$\frac{19.283}{6.250} = 3,08528.$$

- Desafio da página 156.

  Vamos calcular as potências de 10 no módulo 3.663 a partir de 4, que é o valor que supera 3.663:

  $$\begin{aligned} 10^4 &\equiv 2.674 \pmod{3.663} \\ 10^5 &\equiv 1.099 \pmod{3.663} \\ 10^6 &\equiv 1 \pmod{3.663}, \end{aligned}$$

  logo o período de $\frac{1}{3.663}$ é 6.

- Desafio da página 158.

  A função bijetiva que existe entre $\mathbb{N}$ e o conjunto dos números ímpares é dada pela fórmula $f(n) = 2 \cdot n + 1$, cujo gráfico é o da figura 3.10.

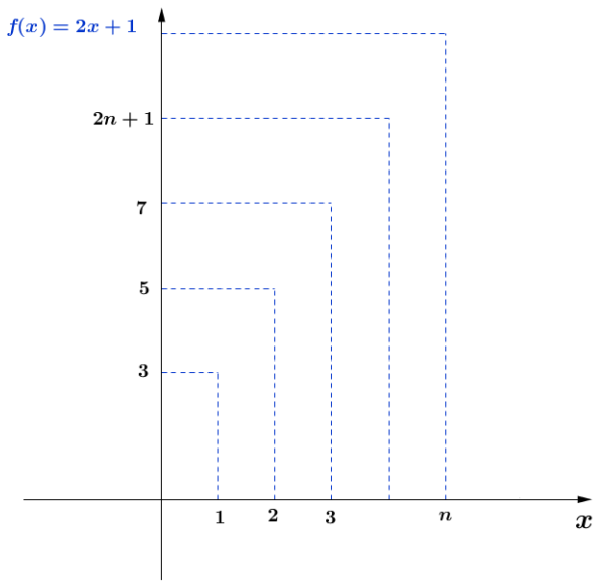


FIGURA 3.10: A bijeção entre os números naturais e os números ímpares.

- Desafio da página 159.

$$
\begin{array}{|rcrcr|}
\hline
\mathbb{N} & \to & \mathbb{Z} & & \\
1 & \to & -\lfloor \frac{1}{2} \rfloor & = & 0 \\
2 & \to & \lfloor \frac{2}{2} \rfloor & = & 1 \\
3 & \to & -\lfloor \frac{3}{2} \rfloor & = & -1 \\
4 & \to & \lfloor \frac{4}{2} \rfloor & = & 2 \\
5 & \to & -\lfloor \frac{5}{2} \rfloor & = & -2 \\
6 & \to & \lfloor \frac{6}{2} \rfloor & = & 3 \\
7 & \to & -\lfloor \frac{7}{2} \rfloor & = & -3 \\
8 & \to & \lfloor \frac{8}{2} \rfloor & = & 4 \\
9 & \to & -\lfloor \frac{9}{2} \rfloor & = & -4 \\
10 & \to & \lfloor \frac{10}{2} \rfloor & = & 5 \\
 & \ldots & & & \\
\hline
\end{array}
$$

- Desafio da página 162 Suponha $r = \frac{s}{t}$ com $\mathrm{MDC}(s,t) = 1$ Temos que

$$r^n = \frac{p}{q} \quad \text{se e somente se} \quad \left(\frac{s}{t}\right)^n = \frac{p}{q},$$

de onde temos que $q \cdot s^n = p \cdot t^n$. Assim, devemos ter que $s \mid p \cdot t^n$ e $t \mid q \cdot s^n$. Como temos $\mathrm{MDC}(s,t) = 1$, então $\mathrm{MDC}(s^n,t) = 1$ e também $\mathrm{MDC}(s,t^n) = 1$, então, pelo lema de Euclides (veja na seção 1.7 do módulo I, a proposição 1.12, pg.67) $s \mid p$ e $t \mid q$.

Concluímos que, se existirem números racionais que verifiquem $r^n = \frac{p}{q}$, devem ser frações cujos numeradores sâo divisores inteiros de p e os denominadores são divisores inteiros de q.

Para finalizar o desafio, vamos encontrar os números racionais r tal que $r^2 = \frac{9}{4}$. Pelo que concluímos, devemos ter $r = \frac{s}{t}$ com $s \mid 9$ e $t \mid 4$. Mas como queremos que r seja irredutível, devemos ter $\frac{3}{2}$ ou $\frac{-3}{2}$, as duas soluções do problema.

Módulo 4
O conjunto dos Números Reais

No término do módulo IV, o aluno estará familiarizado como os seguintes conceitos:

- ▷ Noções gerais sobre a representação decimal de números reais.
- ▷ A não enumerabilidade dos números reais.
- ▷ Os números irracionais.

Introdução

O conceito de número real ou **reta real** são usados desde o ensino médio e chegando à universidade suas propriedades são exploradas nos cursos de cálculo. Mas, realmente...

O que é um número real ou a reta real? Qual seria a definição específica destes conceitos? O que realmente são o número π ou o número $\sqrt{2}$?
Suponha que um estudante do ensino médio lhe pede para explicar exatamente o que é um número real. O que você responderia ao aluno?

O objetivo deste módulo é que, depois do estudo e compreensão do mesmo, você possa dar ao seu aluno uma resposta satisfatória para a pergunta: o que é um número real?. Em particular, você deve entender em que sentido o conjunto dos números reais é exatamente o conjunto dos números decimais.

Como motivação, vamos começar estudando a seguinte questão: seja $ABCD$ o quadrado de lado l como na figura 4.1.

Calculando a medida da diagonal em função do lado l obtemos pelo **Teorema de Pitágoras** que

$$d^2 = l^2 + l^2 = 2l^2.$$

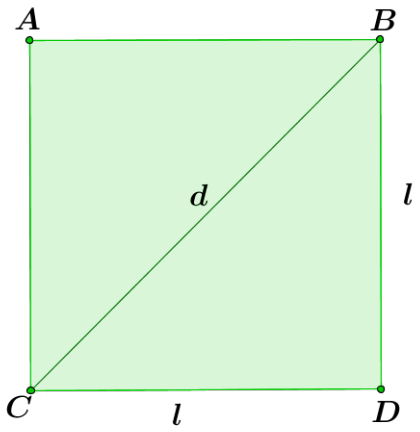


FIGURA 4.1: Quadrado de lado l

Suponha que o comprimento de l é tomado como **unidade de medida**. Então obtemos a expressão

$$d^2 = 2. \tag{4.1}$$

A questão é se o número d solução da equação (4.1) poderia ser um *número racional*.

Esta questão é muito antiga. O primeiro matemático puro reconhecido pelos historiadores foi Pitágoras de Samos (por volta de 569 AC -475 AC), que fundou a escola Pitagórica e cujos seguidores tentaram fazer o cálculo da diagonal de um quadrado de lado 1 como apresentado acima. Porém, não encontravam um valor, número inteiro ou racional (na época conhecida apenas como fração), que representasse o valor da medida de d. A descoberta para essa época foi revolucionária mas também perturbadora, pois contrariava os pensamentos aceitos pela comunidade científica e de fato constituía um ideia nova a ser explorada. Muitos dos seguidores da escola de Pitágoras, chamados de pitagóricos, esconderam essa descoberta por medo do impacto na sociedade da época. Foi um "segredo" até que o matemático grego Hipaso de Metaponto (por volta de 500 AC) a fez pública. Conta a lenda que essa divulgação foi feita em um navio e foi jogado no mar por incrédulos fanáticos. Outros afirmam que ele foi banido da escola e da comunidade pitagórica.

Vamos demonstrar que, de fato, a equação (4.1) não tem solução que seja um número racional. A forma de demonstrar essa afirmação é pelo absurdo, supondo que existe d, número racional, que verifica (4.1). Vamos tomar $d = \frac{a}{b}$ o representante irredutível com $b > 0$. Assim,

usando (4.1) obtemos

$$\left(\frac{a}{b}\right)^2 = 2 \quad \text{ou equivalentemente} \quad a^2 = 2 \cdot b^2. \tag{4.2}$$

Deduzimos da segunda igualdade em (4.2) que $2 \mid a^2$. Portanto temos que $2 \mid a$. Assim temos

$$a = 2 \cdot k, \quad \text{para algum } k \text{ inteiro.} \tag{4.3}$$

Voltando à segunda igualdade em (4.2), vamos substituir a escrito como em (4.3), obtendo

$$\begin{array}{l} (2 \cdot k)^2 = 2 \cdot b^2 \quad \text{ou equivalentemente} \\ 4 \cdot k^2 = 2 \cdot b^2 \quad \text{e dividindo por 2 obtemos} \\ 2 \cdot k^2 = b^2. \end{array}$$

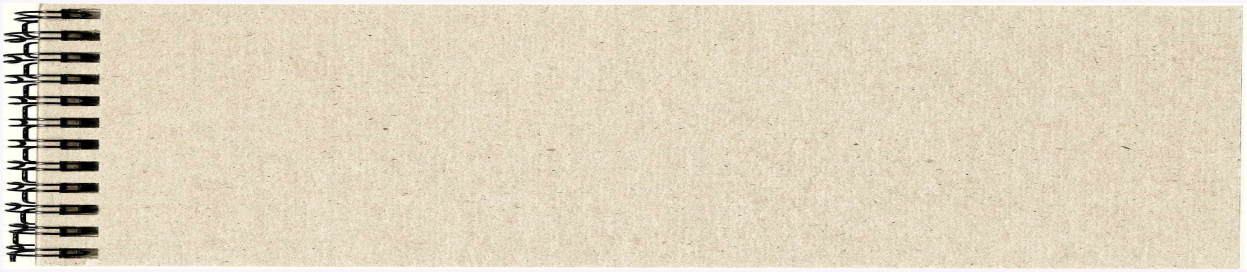
Esta última igualdade confirma que $2 \mid b^2$ e portanto $2 \mid b$. Ou seja, concluímos que o MDC(a, b) é pelo menos 2. Isto é uma contradição com o fato de que $\frac{a}{b}$ é uma fração irredutível.

Este mesmo procedimento pode ser usado para mostrar que não existe d, número racional, tal que

$$d^2 = p \text{ onde } p \text{ é um número primo (veja módulo I, definição 1.28, pg.74)} \tag{4.4}$$

Desafio!

Prove que não existe um número racional tal que r tal que $r^2 = 5$.



Clique aqui para ver a resposta.

A solução da equação (4.1) é denotada por $\sqrt{2}$.

Observação 4.1. Note que o elemento $\sqrt{2}$ não pertence a $\mathbb{Q}$ e verifica

$$\sqrt{2} > x \quad \text{para todo número racional} \quad x \quad \text{tal que} \quad x^2 \leq 2. \tag{4.5}$$

Do ponto de vista da representação dos números racionais na reta orientada, o fato de $\sqrt{2}$ não ser um número racional significa que a reta tem um "furo", mesmo que os números racionais tenham a propriedade de densidade (veja módulo III, proposição 3.5, pg.142). Esta interpretação geométrica está ilustrada na figura 4.2.

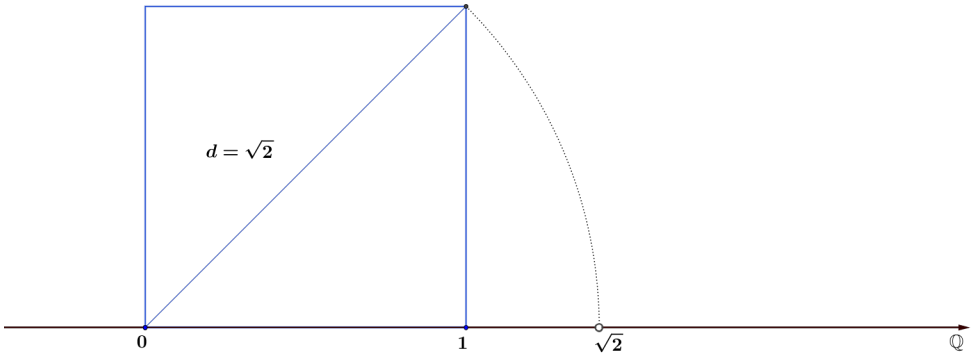


FIGURA 4.2: O ponto $\sqrt{2}$ é um "furo" na reta racional.

A impossibilidade de escrever os números da forma (4.4) como um número racional deu lugar a novos números: os irracionais. Grandes matemáticos ao longo da história trabalharam este conceito. Foi o matemático alemão Richard Dedekind (1831-1916) que apresentou a teoria dos números irracionais com rigor. Iremos estudar um pouco mais sobre estes números na seção 4.3.

Matemáticos como Augustin Louis Cauchy (1789-1857), Dedekind, Karl Weierstrass (1815-1857), Georg Cantor (1845 – 1918), entre outros, tentaram fazer um enfoque que não envolvesse geometria, forma como foi tratado o problema da irracionalidade por muitos séculos. Assim surgiram várias formas teóricas de construir os números reais: as Sequências de Cauchy, a teoria dos Intervalos Encaixantes, os Cortes de Dedeking, entre outras. Na seção 4.1 iremos estudar a construção por representação decimal dos números reais. Na seção 4.4 iremos apresentar uma resenha das construções acima mencionadas.

Note que historicamente houve uma "necessidade" de uma formalização da ideia da irracionalidade e de fundamentar a existência do conjunto dos números reais como um conjunto "completo" em algum sentido específico.
Completar o conjunto dos racionais para que a reta não tenha furos não foi, porém, uma tarefa fácil teoricamente.
A questão para pensar é por que na escola usamos as expressões decimais para trabalhar os números reais. O que elas possuem de importância teórica para serem utilizadas desde tão cedo?

Uma outra questão teórica a ser levantada é se todas essas construções criadas levam a definir o mesmo conjunto de números, aquele a que chamamos de conjunto dos números reais.

Axiomaticamente falando, um conjunto de números reais deve satisfazer algumas propriedades que caracterizam este conjunto. Isto é feito através da definição de um sistema de axiomas.

Os conceitos primitivos do sistema de axiomas são pontos (números reais), as operações de adição e multiplicação, e uma relação de ordem. As propriedades que descrevem estas operações são similares às que satisfazem as operações de adição e multiplicação no conjunto dos números racionais. A única exceção é o axioma de completude, que é justamente aquele que se refere a que não há "buracos" na reta real. Nós nos referimos a qualquer modelo para o sistema de axiomas, o correspondente ao corpo dos números reais.

Há dois fatos importantes que justificam o uso das expressões *reta real* ou *corpo dos números reais*. Primeiramente, existem modelos concretos onde o sistema de axiomas pode ser verificado. Em segundo lugar, todos os modelos que satisfazem o sistema de axiomas são isomorfos, o que significa matematicamente que possuem *a mesma estrutura*. Mais precisamente, pode ser estabelecida uma função bijetiva f entre dois conjuntos de números construídos de maneira diferente, de forma que f preserva a adição, multiplicação e a ordem estabelecidas nesses conjuntos. Em outras palavras, só existe teoricamente uma única reta real ou um único corpo dos números reais. Então...se este é verdadeiro...

Qual é o sistema de axiomas que caraterizam os números reais?

Os axiomas vêm em três "pacotes" correspondentes à aritmética, a uma ordem estabelecida entre os objetos e à completude, conceito que será especificado. Os axiomas em conjunto afirmam que o conjunto dos números reais é um corpo, ordenado e completo.

Enunciamos a seguir o primeiro pacote de axiomas.

Axioma 1 (Axiomas de Corpo)**.** Um corpo é um conjunto C de elementos munido de duas operações binárias, $+$ e $\cdot$ que verificam as propriedades associativa, comutativa, existência e unicidade de neutro e simétrico, excetuando o neutro da operação $+$ que não tem simétrico (veja módulo III, observação 3.3, pg. 139).

Note que as propriedades da adição e multiplicação são comuns às das operações definidas no conjunto dos números racionais (veja módulo III, proposição 3.1 e proposição 3.2).

O segundo pacote do sistema de axiomas vem dado pelos axiomas de ordem a seguir.

Axioma 2. *(**de Ordem**)* Um corpo $(C, +, \cdot)$ onde está definida uma relação de ordem $>$ em C verificando:

- Tricotomia: Dados dois elementos diferentes $c_1,\ c_2 \in C$ tem-se uma só uma das possibilidades $c_1 > c_2$ ou $c_2 > c_1$.
- Transitiva: se $c_1 > c_2$ e $c_2 > c_3$, então $c_1 > c_3$, para todo $c_1,\ c_2$ e $c_3 \in C$.
- A relação de ordem $>$ é compatível com as operações definidas em C no sentido que se $c_1 > c_2$ então $c_1 + c > c_2 + c$, para todo $c \in C$. Se $c_1 > c_2$ e $0 < c$, temos que $c_1 c > c_2 c$ e, finalmente, se $c_1 > c_2$ e $c < 0$, então devemos ter $c_2 c > c_1 c$.

Os axiomas deste segundo pacote são os que caracterizam um **corpo ordenado**  . Vimos que o conjunto dos números racionais, da forma que foi construido no módulo III (veja seção 3.1), também verificam a axiomática de ordem.

Há outra importante propriedade de ordenação dos números reais que não pode ser obtida diretamente a partir dos outros axiomas de ordem enunciados no Axioma de ordem de Arquimedes. Este axioma está relacionado com a propriedade arquimedeana, demonstrada para a ordem estabelecida no conjunto dos números racionais (veja no módulo III, subseção 3.1.2, pg.137).

Axioma 3 (Axioma de Ordem de Arquimedes)**.** Seja um corpo corpo $(C, +, \cdot)$ ordenado pela relação $>$ e $a > 0$ e $b > 0$, elementos do corpo. Então existe um inteiro $n_0 > 0$ tal que $n_0 a > b$.

Quando um corpo ordenado satisfaz o axioma de ordem de Arquimedes, é chamado de corpo arquimedeano.

Observação 4.2. Note que, se tomarmos $a = 1$ no axioma ordem de Arquimedes 3, vemos que, para cada $b > 0$, existe um inteiro positivo n_0 tal que $n_0 a = n_0 > b$, ou seja, o conjunto $\{n \in \mathbb{N}, n > b\}$, não é vazio e, pelo Princípio de Boa Ordenação (veja no módulo I, teorema 1.1, pg. 39), existe um número natural m, mínimo desse conjunto. Além disso, temos que $0 \leq m - 1 < b < m$.

Até agora temos revisado propriedades das operações e da relação de ordem que já foi visto no conjunto dos números racionais.
Pois então, qual é a diferença em termos de estrutura entre o conjunto dos números racionais e dos números reais?

Já notamos a necessidade geométrica da construção dos números reais, na reta racional, que está "cheia" de furos. Vamos dar a seguir um fundamento teórico de como resolver este problema geométrico.

Neste sentido segue o terceiro pacote de axiomas do sistema de axiomas que caracteriza o conjunto dos números reais, que é o mais destacado deste conjunto por estar relacionado com a falta de furos na reta real.

Axioma 4 (Completude: Axioma de Dedekind)**.** Um corpo $(C, +, \cdot)$ ordenado é dito completo se todo subconjunto de C limitado superiormente possui supremo.

Lendo o enunciado do axioma de Dedekind, não aparece claro que tenha ver esse enunciado com o fato de prencher a reta racional para ter uma reta real "totalmente" cheia. Veremos um pouco mais para frente como o axioma de Dedekind explica isto. Mas antes, vamos esclarecer o que significam os conceitos envolvidos no axioma, como são os conceito de conjunto limitado e de supremo.

Definição 4.1. *Seja $A \subset C$ onde C é um conjunto com uma relação de ordem.*

1. *O conjunto A é dito limitado superiormente se existir $s \in A$ tal que $a \leq s$ para todo $a \in A$. O elemento s é dito cota superior de A.*
2. *Uma cota superior de A, s_0, é o supremo de A se $s_0 \leq s$, para todo $s \in C$, cota superior de A. Ou seja, o supremo de A é* a menor das cotas superiores.

Associado aos conceitos enunciados na definição 4.1 temos os conceitos análogos para limitação inferior, como enunciado na seguinte definição.

Definição 4.2. *Seja $A \subset C$ onde C é um conjunto com uma relação de ordem.*

1. *O conjunto A é dito limitado inferiormente se existir $i \in A$ tal que $a \geq i$ para todo $a \in A$. O elemento i é dito cota inferior de A.*
2. *Uma cota inferior de A, i_0, é o ínfimo de A se $i_0 \geq i$, para todo $i \in C$, cota inferior de A. Ou seja, o ínfimo de A é* a maior das cotas inferiores.
3. *Quando o conjunto A é limitado superiormente e inferiormente, diz-se que A é limitado.*
4. *Um elemento é máximo do conjunto A se possui supremo s_0 e tem-se $s_0 \in A$.*
5. *Um elemento é mínimo do conjunto A se possui ínfimo i_0 e tem-se $i_0 \in A$.*

Exemplo 4.1. Considere o conjunto $A = \{\frac{1}{2}, -4, 0, 4\}$. Temos que qualquer número $x \leq -4$ é cota inferior de A. Isto faz, por definição, que -4 é ínfimo do conjunto A. Como temos $-4 \in A$, então -4 é mínimo de A.
Da mesma forma, todo $x \geq 4$ é cota superior de A, concluindo que 4 é supremo de A e, por pertencer a A, também é máximo de A.

Desafio!

Determine cotas superiores, inferiores do conjunto $A = \{x = \frac{1}{n},\ n \in \mathbb{N}\}$. Este conjunto tem supremo, ínfimo? E máximo, mínimo?

Clique aqui para ver a resposta.

Agora explicaremos como o axioma de Dedekind se refere aos furos da reta racional. Preste atenção ao seguinte exemplo!

Exemplo 4.2. Considere o conjunto dos números racionais

$$A = \{x \in \mathbb{Q}, x^2 \leq 2\}.$$

Temos que 3 é cota superior de A, pois $x^2 \leq 2 < 3^2$, portanto $x^2 < 3^2$, de onde $x < 3$, para todo $x \in A$. Também observamos que -3 é cota inferior de A, pois, se fosse $-3 > x$, então, elevando ao quadrado, obtemos $x^2 > 9$. Veja a figura 4.3 ilustrando o conjunto A.

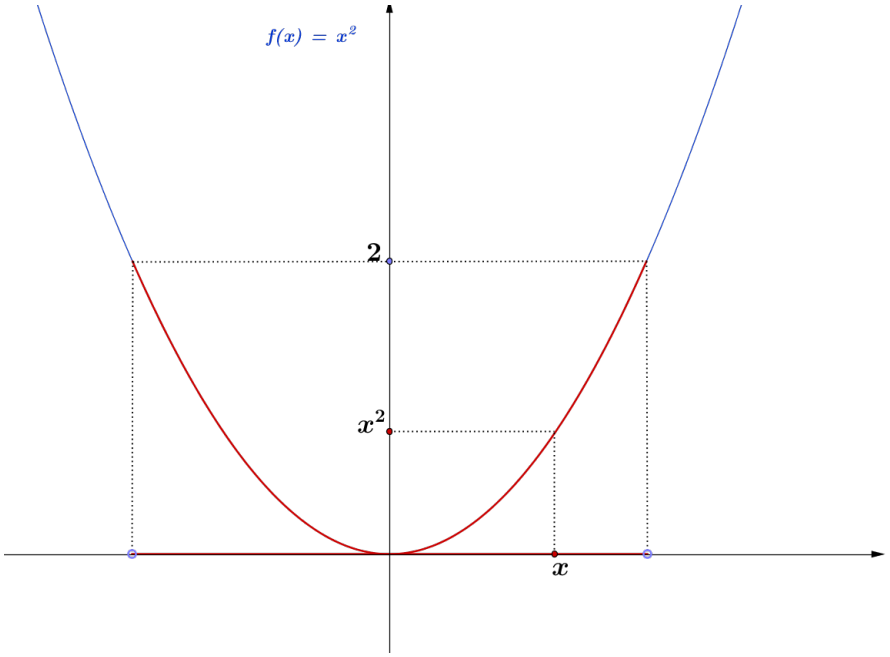


FIGURA 4.3: O conjunto A representado em cor vermelha sobre o eixo $0x$.

Exemplo 4.3. Dado o conjunto

$$E = \{x \in \mathbb{Q},\ x < 1\}$$

tem como supremo o número 1 pois toda cota superior é maior ou igual a 1. O conjunto E não tem cotas inferiores e, em consequência, não tem ínfimo.
Note que o supremo de E não pertence ao conjunto!

Com o objetivo de praticarmos com o conceito de supremo, vemos uma das suas propriedades que tem a ver com o conjunto soma de dois conjuntos. A seguir, definimos este conceito e demonstramos a propriedade em questão.

Definição 4.3. *Dados dois conjuntos de números, A e B, definimos o conjunto soma desses conjuntos e denotamos por $A + B$ como*

$$A + B = \{x = a + b,\ a \in A,\ b \in B\}, \tag{4.6}$$

ou seja, é o conjunto formado por todas as somas possíveis dos elementos de A e B.

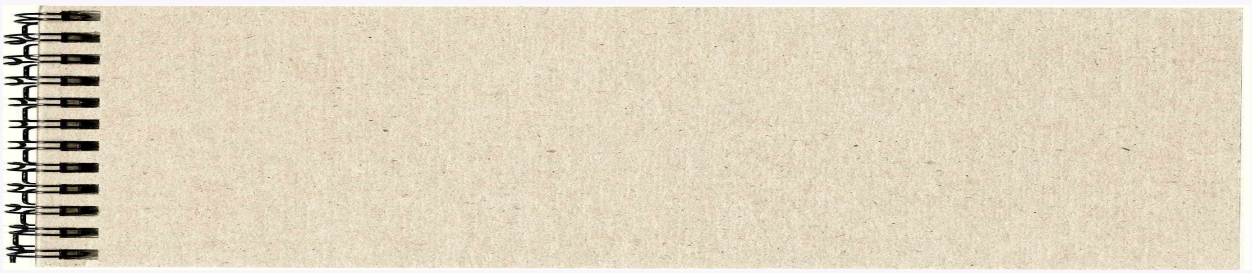
Entendeu a definição? Então vamos praticar!

Desafio!

Considere os conjuntos

$$A = \{1, -1, 3\} \quad \text{e} \quad B = \{0, 1, 2\}$$

Anote no caderno o conjunto soma de $A + B$.



Clique aqui para ver a resposta.

Proposição 4.1. *Considere um corpo C ordenado e $A \subset C$ e $B \subset C$ e suponha que existem os supremos de ambos os conjuntos. Então o conjunto $A + B$ é limitado superiormente e se o supremo $A + B$ existir, tem-se*

$$\sup(A + B) = \sup(A) + \sup(B), \tag{4.7}$$

onde $\sup()$ é a notação para o supremo de um conjunto.
Em outras palavras, a proposição afirma que o supremo da soma é a soma dos supremos.

Demonstração: Seja s_A o supremo de A e s_B o supremo de B. Pela definição 4.1 temos que

$$a \leq s_A, \quad \text{para todo } a \in A,$$

e da mesma maneira

$$b \leq s_B, \quad \text{para todo } b \in B.$$

Assim, como estamos em um corpo ordenado, verifica-se a propriedade de monotonia da soma (veja o axioma 2, pg. 172), obtendo como consequência

$$a + b \leq s_A + s_B, \quad \text{para todo } a \in A \text{ e } b \in B. \tag{4.8}$$

A desigualdade (4.8) mostra que o conjunto $A + B$ tem como uma cota superior $s_A + s_B$, portanto é limitado superiormente. Suponha que existe $s_{A+B} = \sup(A + B)$, então, de (4.8) e do fato de que $s_A + s_B$ é uma cota superior, pode-se concluir que

$$s_{A+B} \leq s_A + s_B. \tag{4.9}$$

Supondo que

$$s_{A+B} < s_A + s_B, \tag{4.10}$$

obtemos que $-s_{A+B} > -(s_A + s_B)$, portanto, somando a ambos os membros $2s_{A+B}$, obtém-se

$$s_{A+B} < 2s_{A+B} - (s_A + s_B). \tag{4.11}$$

De (4.10) temos que $s_{A+B} - s_A < s_B$ e portanto $s_{A+B} - s_A$ não pode ser cota superior de B, e assim existe b_0 tal que

$$s_{A+B} - s_A < b_0 \leq s_B. \tag{4.12}$$

Da mesma maneira obtemos a existência de a_0 tal que

$$s_{A+B} - s_B < a_0 \leq s_A. \tag{4.13}$$

Assim, somando membro a membro (4.12) e (4.13) e usando a desigualdade (4.10), obtemos

$$s_{A+B} < 2s_{A+B} - (s_A + s_B) < a_0 + b_0 \in A + B,$$

o que é uma contradição, pois s_{A+B} é supremo de $A + B$. ■

Observação 4.3. Note que na proposição 4.1 foram usados os axiomas de corpo ordenado e algumas propriedades que se deduzem deles, como é afirmação a seguir,

$$\text{se } x > y \quad \text{então } -y > -x,$$

isto é, os opostos de dois elementos de um corpo estão na relação de ordem oposta.

Voltando para o conjunto dos números racionais, vamos ver que, no exemplo 4.2, o conjunto A não possui supremo. Isto será demonstrado na seguinte proposição.

Proposição 4.2. *O conjunto $\mathbb{Q}$ dos números racionais não verifica o axioma de Dedekind.*

Demonstração: O conjunto $A = \{x \in \mathbb{Q}, x^2 \leq 2\}$ não possui supremo que pertença a $\mathbb{Q}$. Note que o supremo "deveria" ser $\sqrt{2}$ que, já vimos na observação 4.1, equação (4.5), não é um número racional. ■

A proposição 4.2 mostra que $\mathbb{Q}$ não verifica o axioma de completude, sendo esta uma das razões já salientadas como a mais importante para a necessidade da construção de um conjunto de números "além" do conjunto dos números racionais.

4.1 Noções Gerais da Representação Decimal dos Números Reais

Vamos definir números reais como o conjunto dos elementos da forma

$$\begin{aligned}
&10,000000000000000000000000000000000000000000\ldots, (=10)\\
&342,200000000000000000000000000000000000000000\ldots, (=\tfrac{3.422}{10})\\
&0,333333333333333333333333333333333333333333\ldots (=\tfrac{1}{3}),\\
&3,141592653589793238462643383279502884197169 39\ldots (=\pi),
\end{aligned}$$

ou seja, os números representados por uma expressão do tipo

$$z, a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}a_{12}a_{13}a_{14}\ldots, \tag{4.14}$$

onde a_i são *dígitos* e z um número inteiro na sua expressão decimal.

Vamos formalizar esta construção seguindo as ideas de Timothy Gowers ([4] nas referências bibliográficas de leitura complementar).

Vamos associar à expressão depois da vírgula em (4.14) uma "lista" de dígitos extraída do conjunto $D = \{0, 1, ..., 9\}$. Esta lista é, teoricamente, uma função de domínio $\mathbb{N}$ e com imagem em D definida por

$$f(n) = a_n \in D, \quad \text{para todo } n \in \mathbb{N}, \tag{4.15}$$

Pela definição feita no módulo I (veja definição 1.2, pg. 20) é uma sequência de dígitos decimais.

Desta forma, a representaçao (4.14) com $a_0 = 0$ é formalmente a sequência

$$a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, \ldots, a_n, \ldots\}.$$

Neste sentido trabalharemos os elementos "infinitos" da expressão (4.14), quando necessário.

Definição 4.4. *O conjunto dos números reais, que denotamos por* $\mathbb{R}$ *é definido como segue:*

$$\mathbb{R} = \{x = z, a_1 a_2 \ldots a_n \ldots,\ a_n \textit{ sequência de dígitos decimais},\ z \in \mathbb{Z}\}, \tag{4.16}$$

onde z *também está expresso na sua forma decimal.*

Devemos esclarecer que a definição 4.4 não é completa. Há algumas "sutilezas" teóricas que devemos discutir.
O objeto $1,9999999\ldots$ é o mesmo número que o número racional 2. Ou, ainda mais geralmente, identificamos os números

$$z - 1,9999999999999\ldots = z,00000000000\ldots.$$

Isto pode ser tomado como uma definição ou também pode-se entender que esses dois números como equivalentes, assim como são equivalentes os números racionais $(2,3)$ e $4,6)$ (veja módulo III, definição 3.1, pg.129).
De acordo com o rigor da construção, ambas as alternativas teóricas aparecem satisfatórias, até para o mais exigente matemático.

Pense na seguinte questão: de que forma identificaremos os números inteiros e racionais na definição 4.4?

Note que primeiramente temos que pensar esses números na sua representação decimal, para manter a coerencia até na notação!

Lembre que vimos no módulo I (teorema 1.3, pg.61) sobre representação decimal de um número inteiro. Também no módulo III (veja seção 3.2, pg.142), obtivemos construtivamente a representação decimal de um número racional, **dízima** finita ou periódica.

A forma de "incluir" os números inteiros no conjunto $\mathbb{R}$ é definindo uma função f_1 entre $\mathbb{Z}$ e $\mathbb{R}$

tal que se $z \in \mathbb{Z}$ vem dado pela representação decimal $z = b_1 b_2 \dots b_m$, então o correspondente real pela função f é

$$f_1(z) = z, 0000 \dots, \tag{4.17}$$

ou seja, a sequência de dígitos é composta só por zeros.

Continuando com a identificação dos números racionais dentro do conjunto $\mathbb{R}$, definimos a função f_2 de $\mathbb{Q}$ em $\mathbb{R}$ tal que para $r = \frac{a}{b} \in \mathbb{Q}$ corresponde o real cuja representação decimal vem dada por

$$f_2(r) = q, a_1 a_2 \dots a_m \overline{c_1 c_2 \dots c_n 00 \dots}, \tag{4.18}$$

onde q é o quociente da divisão inteira de a por b e, a_i e c_i, os dígitos da representação decimal de r.

Isto completa a identificação dos números inteiros e racionais "dentro" do conjunto dos números reais definidos como o conjunto de todos os decimais.

Gostaríamos a seguir tornar $\mathbb{R}$ um corpo ordenado e completo. Portanto, devemos passar para as definições de adição e multiplicação, assim como estabelecer uma ordem que verifique todos os axiomas 1,2,3,4.

A primeira questão é: como é que vamos adicionar dois números decimais infinitos?

Esta dificuldade para definir adição de dois elementos de $\mathbb{R}$ é uma das razões do porquê as teorias mais sofisticadas "ganham" desta, mais intuitiva, nos cursos de nível superior. Mas... como continuar a teoria sem perder a intuição?

A primeira tentativa seria seguir o mesmo procedimento que faríamos para somar números decimais finitos, que não são outros que os praticados nos anos de escola e ensino médio. Mostraremos os inconvenientes teóricos para estes procedimentos para o conjunto dos decimais infinitos.

Suponha que temos dois números reais cuja sequência de dígitos não é zero ou 9 a partir de um natural n dado em diante. Chamaremos a este decimal não periódico. Um número real desse tipo é

$$a = 3, 14159265358979323846264338327950288419716939 \dots,$$

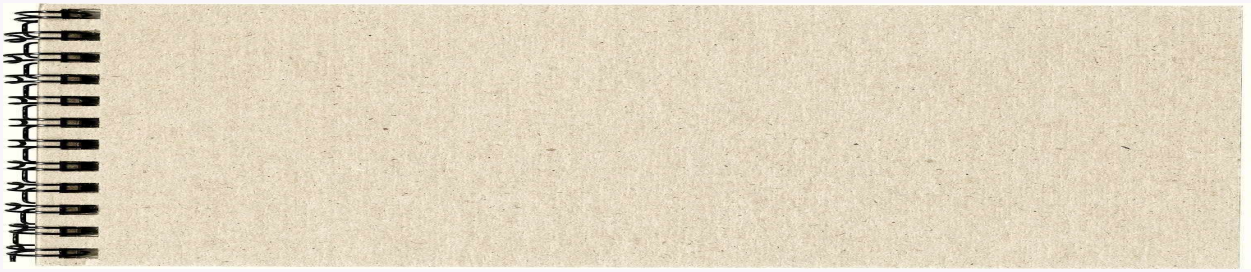
como mostrado no começo desta seção.

A questão é: como fariamos para somar esse número a um número do tipo

$$b = 5, 2231020020002000020000020000002000000020000000002 \dots ?$$

Desafio!

Você descubriu a lei de formação do número b? Anote sua conclusão.



Clique aqui para ver a resposta.

Observe que, se quisermos somar da forma que é feita para decimais finitos, teríamos que começar somando os dígitos que estão no extremo direito dos somandos que, em ambos os casos de nosso exemplo, esses extremos não existem, já que a sequência de dígitos "não tem fim", é infinita.

Uma alternativa para este inconveniente seria começar a somar pela esquerda. No exemplo, para efetuar $a + b$, somaríamos as partes inteiras $3 + 5$ e esse será nosso primeiro dígito à esquerda da soma. Continuando o procedimento, obteríamos até a casa decimal 18 que

$$\begin{array}{r} 3,141592653589793238\ldots \\ + \\ 5,223102002000200002\ldots \\ \hline 8,364694655899932310\ldots \end{array}$$

Ou seja, no lugar 18 da sequência dos dígitos da soma de a e b, teríamos que colocar 0 e "levar" um para o lugar 17 da sequência para "ajustar" o resultado. Com muita paciência poderíamos repetir esses ajustes nos seguintes passos do procedimento de adicionar dois números reais, desta maneira, porém, ainda com o inconveniente de que o processo "não tem fim", é infinito.

Como dar a volta por cima deste inconveniente técnico?

A resposta é simples. Porém, para explicá-lo de forma mais clara, vamos fazer algumas definições, aparentemente muito técnicas mas muito mais intuitivas. Primeiramente, vamos combinar uma notação que facilita nossas demonstrações.

Notação 4.1. *Os números reais correspondentes por f_2 (veja 4.18) aos racionais decimais finitos, isto é, da forma*

$$z, a_1, a_2, \ldots a_n 0000 \ldots,$$

ou, equivalentemente,

$$z, a_1, a_2, \ldots (a_n - 1)9999999999 \ldots,$$

os denotaremos como $z, a_1, a_2, \ldots a_n$, ou seja, sem o zeros (ou os noves) que contêm a correspondente sequência de dígitos.

Definição 4.5. *Seja um número real $x = z, a_1 a_2 \ldots a_n \ldots$, onde $\{a_1, a_2, \ldots\}$ é uma sequência de dígitos e z é um inteiro representado em forma decimal.*

$$x(n) = z, a_1 a_2 \ldots a_n \ldots 000000 \ldots$$

é chamado de truncamento do número real com n dígitos decimais, ou simplesmente, de ordem n, do número x.
Diz-se que a sequência definida por

$$f(n) = x(n), \quad \text{denotada por} \quad \{x(n)\},$$

é a sequência dos truncamentos de x.

Exemplo 4.4. Dado o número

$$3, 14159265358979323846264338327950288419716939 \ldots,$$

temos que, usando a notação 4.1

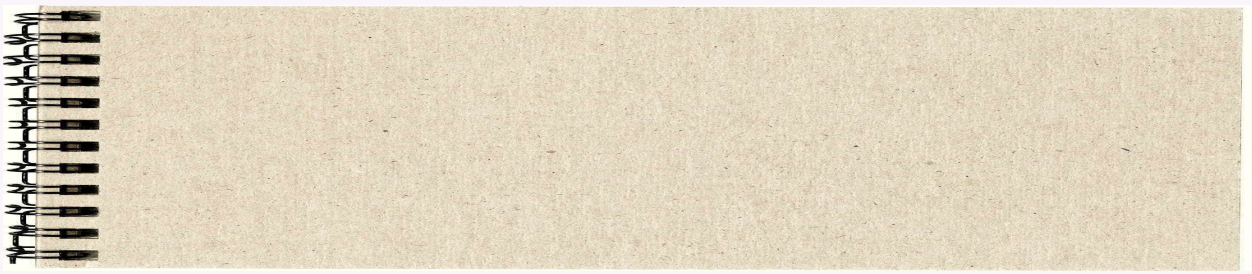
$$\begin{aligned} x(1) &= 3, 1; \\ x(2) &= 3, 14; \\ x(10) &= 3, 1415926535, \end{aligned}$$

a sequência de truncamentos é dada pela lista infinita

$$3, 1;\ 3, 14;\ 3, 141; \ldots.$$

Desafio!

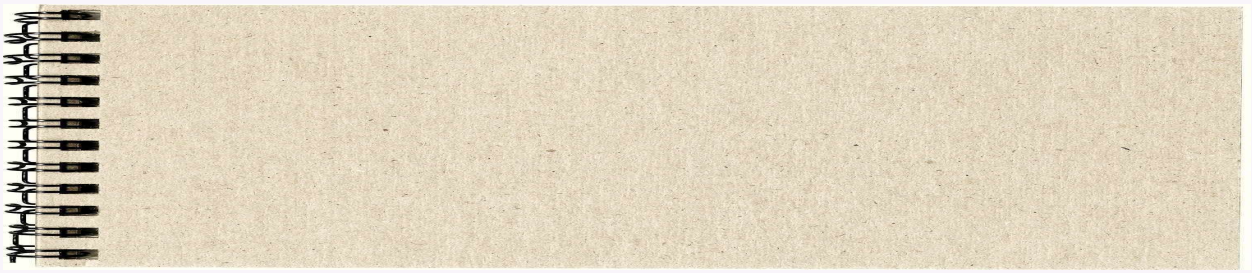
Usando a calculadora, ache o truncamento de ordem 10, $x(10)$, de $\sqrt{5}$.



Clique aqui para ver a resposta.

Desafio!

Usando a calculadora, escreva a sequência de truncamentos do número real $\sqrt{2}$ até o truncamento de ordem 15.



Clique aqui para ver a resposta.

Definimos então a adição no conjunto 4.4.

A operação de adicionar dois números reais x e y na sua representação decimal se reduze a considerar a sequência de decimais finitos $\{x(1)+y(1), x(2)+y(2), \ldots, x(n)+y(n), \ldots\}$.

Por exemplo somando os números

$$3,14159265358979323\textcolor{red}{8}\ldots$$

e

$$5,22310200200020000\textcolor{red}{2}\ldots,$$

a sequência de truncamentos da soma seria

$$8,3;\ 8,36;\ 8,364;\ 8,3646;\ 8,36469;\ 8,364694;\ 8,3646946;\ldots\},$$

Como observamos nas nossas primeiras considerações, alguns dos dígitos da expressão $x(n)+y(n)$ precisam ser modificados porque a soma dos dígitos seguintes pode não ser um dígito, ou seja, um número inteiro entre 0 e 9. Porém, é fácil ver que nenhum dígito é sempre

modificado mais do que uma vez. Isto leva à conclusão de que esta definição é conveniente para lidar com o "infinito".

Uma outra forma de tentar formalizar o conceito de adição no conjunto dos números reais constituído por decimais é a de definir uma noção de limite, porque no final estamos tratando com elementos infinitos (as sequências de truncamentos) e queremos nos aproximar de uma expressão também do tipo infinito (o número real que não é racional).

Como o aluno que faz este curso está familiarizado com o conceito de limite nos cursos de cálculo, vamos explorar esta forma de fundamentar melhor a teoria, sem abandonar a intuição que viemos trabalhando até o momento.

Como primeiro passo, vamos definir uma ordem no conjunto dos números reais decimais, que não é outra que a usada comumente para comparar decimais gerados por números racionais. Lembre que a intenção é que a função (4.18) preserve a estrutura de $\mathbb{Q}$!

Só para introduzir a ideia, mesmo que bem conhecida, a forma de comparar dois números reais positivos como

$$a = 0,813656101101110... \qquad b = 0,8139666101101110...$$

é comparar os dígitos começando pela esquerda. Note que os três dígitos de a e b coincidem depois da vírgula, mas o quarto dígito de a é 6 enquanto de b é 9. Assim $b > a$. Esta relação de ordem leva o nome de ordem lexicográfica, pois segue a mesma regra da ordem das palavras do dicionário. A ordem em que aparecem as letras é similar a como estão ordenados os dígitos $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$.

Qual é a palavra que no dicionário aparece primeiro: demonstração ou demonstrado? Note que as duas palavras coincidem até a letra "ç", em que a palavra demonstrado troca pela letra d. Mas, como a letra ç é anterior à letra d no alfabeto, temos que a palavra demonstração aparece primeiro no dicionário!

Só que vamos ter que ter cuidado para não usar esta ordem para comparar duas representações decimais diferentes correspondentes ao mesmo número. De fato, para os números $a = 0,999999999...$ e $b = 1,0000000000...$ que são na realidade o mesmo número, se aplicarmos a ordem lexicográfica, concluiríamos que $a < b$ pois o primeiro dígito de a antes da vírgula é 0 enquanto o do b é 1.

Vamos então estabelecer uma relação de ordem em $\mathbb{R}$ seguindo a ordem lexicográfica. Dados dois números reais $x = x_0, x_1x_2 \dots x_n \dots$ e $y = y_0, y_1y_2 \dots y_n \dots$ com x_0 e y_0 inteiros na forma decimal. No caso que x e y são inteiros ou racionais, usamos a relação de ordem esta-

belecida nestes conjuntos, já que gostaríamos de preservar a estrutura de ordem pelas funções (4.17) e (4.18). No caso que x e y são reais não periódicos temos a seguinte definição.

Definição 4.6. *Dados dois números reais não periódicos* $x = x_0, x_1x_2 \ldots x_n \ldots$ *e* $y = y_0, y_1y_2 \ldots y_n \ldots$ *com* x_0 *e* y_0 *inteiros na forma decimal. Diz-se que* $x > y$ *se* $x_0 > y_0$ *ou no caso que* $x_0 = y_0$ *se existir* n_0 *natural tal que*

$$x_n = y_n \quad \text{para todo } n < n_0 \quad \text{e } x_{n_0} > y_{n_0},$$

Exemplo 4.5. O número $x = 345,67890067890006789\ldots$ é maior que $y = 345,67886060060006000 6\ldots$ porque $x_n = y_n$ para $n < 4$ e $x_4 = 9 > 8 = y_4$.

Observação 4.4. Dado um real $x = x_0, x_1x_2 \ldots x_n \ldots$ existe um número real z que pode ser identificado como um número inteiro tal que $x \leq z$. Basta tomar $z = x_0 + 1$.

Uma observação análoga à 4.4 pode ser feita com respeito ao número inteiro x_0. Este número é chamado da parte inteira por defeito de x e $x_0 + 1$ da parte inteira por excesso de x. As propriedades vistas para a parte inteira de um número racional (veja módulo 3, definição 3.6, pg. 150) também são válidas para a parte inteira de um número real.

Volte à observação 4.2. Compare a observação 4.4 com a conclusão feita axiomaticamente.

Definição 4.7. *Seja uma sequência de números reais* $\{r_1, r_2, r_3, \ldots, r_m \ldots\}$ *é dita monótona se uma das possibilidades acontece:*

1. *Para todo* $m \in \mathbb{N}$ *se verifica que* $r_m \geq r_{m+1}$ *(monótona não crescente);*
2. *Para todo* $m \in \mathbb{N}$ *se verifica que* $r_m \leq r_{m+1}$ *(monótona não decrescente).*

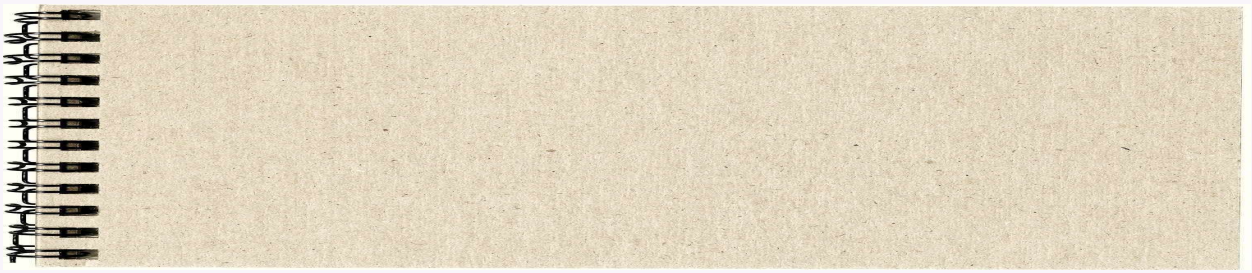
Quando a desigualdade é estrita, diz-se que a sequência é monótona estrita (crescente ou decrescente)

Desafio!

Mostre que a sequência números reais

$$\{3,1;\ 3,14;\ 3,145;\ 3,1415;\ldots\},$$

sequência dos truncamentos do número π é uma sequência de números reais (identificados com números racionais) não decrescente e limitada superiormente.



Clique aqui para ver a resposta.

Exemplo 4.6. *Sejam o números reais π e $\pi - 0,01$. Temos que*

$$\{3; 3,1; 3,14; 3,141; 3,1416; \ldots\},$$

é a sequência de truncamentos do número π e

$$\{3; 3,1; 3,04; 3,041; 3,0416; \ldots\},$$

é a sequência de truncamentos do número $\pi - 0,01$. Note que cada elemento da primeira sequência é menor ou igual que ao correspondente da segunda sequência.

Enunciamos o fato observado no exemplo 4.6 em forma geral na proposição a seguir. Essa afirmação é consequência imediata da definição da relação de ordem no conjunto dos números reais decimais.

Proposição 4.3. *Seja uma sequência não decrescente $\{r_1, r_2, r_3, \ldots, r_m \ldots\}$ de números reais, isto é, se verifica que $r_1 \leq r_2 \leq \ldots \leq r_m \leq \ldots$. Então, para cada n fixado, a sequência de números*

$$\{r_1(n), r_2(n), \ldots, r_m(n) \ldots\}$$

é também não decrescente.

Como consequência imediata da observação 4.4 temos também a seguinte afirmação.

Proposição 4.4. *A sequência de truncamentos de um número real $x > 0$ é monótona (crescente estrita) e limitada superiormente pela parte inteira por excesso de x.*

Nosso objetivo agora é encontrar o supremo (e ínfimo) de conjuntos de números reais limitados. Antes uma observação importante.

Observação 4.5. Note que se um número terminado em zeros é ínfimo de um conjunto então deve pertencer ao conjunto e portanto é o mínimo do conjunto. Analogamente, se um número terminado em noves é supremo de um conjunto, então esse número deve ser seu máximo.

A seguir o teorema que garante a existência do supremo do conjunto dos truncamentos de ordem n de um número real x.

Teorema 4.1. *Seja $X = \{x_1, x_2 \ldots, x_m, \ldots\}$ uma sequência crescente (estrita) de números reais e c é uma cota superior de X. Então existe $x = \sup X$.*

Demonstração: Note primeiramente que, como a sequência é limitada por c, então $\lceil x_m \rceil \leq \lceil c \rceil$. Como a sequência é crescente estrita, então deve existir algum m_0, tal que $\lceil x_{m_0} \rceil = \lceil x_m \rceil$ para todo $m \geq m_0$. Em outras palavras, tendo uma sequência de números inteiros crescente estrita e limitada superiormente, devemos ter essa sequência constante a partir de um elemento da sequência em diante.

Agora consideramos a sequência

$$X_{m_0} = \{x_{m_0}(1) \leq x_{m_0+1}(1) \leq \ldots \leq x_{m_0+k}(1) \leq \ldots\},$$

com $k \in \mathbb{N}$. Assim, pela proposição 4.3 sabemos que é crescente escrita. Portanto, se denotarmos a_n^1 os dígitos depois da vírgula dos elementos da sequência X_{m_0}, então esta sequência é novamente uma sequência de números inteiros crescente estrita e limitada superiormente pelo número 9, logo devemos ter essa sequência constante a partir de um n_1. Seja $a_{n_1}^1$ o primeiro dígito a partir do qual todos são iguais.

Como conclusão obtemos que o número (racional) $\lceil x_{m_0} \rceil, a_{n_1}^1$ que é o supremo da sequência X_{m_0}.

Por indução, suponha que temos

$$\lceil x_{m_0} \rceil, a^1_{n_1} a^2_{n_2} \ldots a^k_{n_k},$$

o supremo da sequência de truncamentos na etapa k do processo indutivo. Sabemos que a sequência dos truncamentos

$$\{x_{m_0}(k+1), x_{m_0+1}(k+1), \ldots, x_{m_0+k+1}(k+1), \ldots\}$$

é monótona crescente estrita e que a sequência dos dígitos que ocupam o lugar $k+1$, que denotamos a^{k+1}_n, é também uma sequência crescente de números inteiros limitada por 9. Então deve existir n_{k+1} natural a partir do qual todos os dígitos a^{k+1}_n são iguais. Seja $a^{k+1}_{n_1}$ o primeiro dígito que verifica essa propriedade.

Então $\lceil x_{m_0} \rceil, a^1_{n_1} a^2_{n_2} \ldots a^k_{n_{k+1}}$ é o supremo da sequência dos truncamentos no passo $k+1$.

Como conclusão do processo indutivo, temos que existe um número real (não necessariamente racional)

$$s = \lceil x_{m_0} \rceil, a^1_{n_1} a^2_{n_2} \ldots a^k_{n_k} \ldots$$

que é o supremo do conjunto X. ■

Como consequência imediata da teorema 4.1 temos o seguinte corolário.

Corolário 4.1. *Seja $x = z, a_1, a_2, \ldots$ um número real. Então temos*

$$x = \sup\{x(n),\ n \in \mathbb{N}\}. \tag{4.19}$$

Observação 4.6. Todas as proposições feitas para o supremo podem ser repetidas com argumentos análogos para o ínfimo.

A importante consequência da proposição 4.1 é que ela fornece uma forma precisa de definir as operações de adição e multiplicação, sem as ambiguidades que encontramos na discussão acima.

Definição 4.8. *Dados os números reais x e y positivos, definimos*

$$x + y = \sup\{x(n) + y(n), n \in \mathbb{N}\}, \tag{4.20}$$

ou seja, como sendo o supremo da sequência crescente e limitada $\{x(1) + y(1), x(2) + y(2), \ldots, x(n) + y(n), \ldots\}$.
Da mesma maneira, definimos $x \cdot y$ como sendo o supremo da sequência crescente e limitada $\{x(1) \cdot y(1), x(2) \cdot y(2), \ldots, x(n) \cdot y(n), \ldots\}$.

As propriedades da adição e multiplicação de números reais positivos podem ser comprovadas facilmente.

A questão a ser resolvida a seguir é: e como definimos números reais negativos? Você sabe responder sem ambiguidade o que é o número $-3,678167811678111678\ldots$?

Uma forma teoricamente fácil, mas que "não combina" com a prática, é pensar cada número real como a soma da sua parte inteira por defeito mais a sua parte decimal "pura", isto é, a sequência dos dígitos que chamamos de mantissa.

Em outras palavras, todo número real x positivo pode ser escrito como

$$x = z + m, \quad \text{onde } z = \lfloor x \rfloor \quad \text{e } m = 0, d_1 d_2 \ldots d_n \ldots. \tag{4.21}$$

A partir desta maneira de ver um número real positivo, definimos o que é um número real negativo. Antes, a definição 4.9.

Definição 4.9. *Definimos como mantissa complementar de m e denotamos por m^c ao número real*

$$m^c = 0, c_1 c_2 \ldots, \text{ com } c_i = 9 - d_i.$$

Note que, da definição 4.9, temos

$$m + m^c = 1.$$

Assim, usando a propriedade de que o conjunto dos números reais positivos é *fechado* com respeito à adição e à multiplicação, podemos estender as operações ao conjunto dos números reais negativos, usando a regra dos sinais. Vamos então definir o que seria o oposto de um número real positivo $x = z + m$.

Definição 4.10. *Seja x um número real positivo $x = z + m$. Definimos o número real $-x$ como*

$$-x = -(z+1) + m^c.$$

Note que da definição 4.10 obtemos imediatamente:

$$x + (-x) = z + m + (-(z+1) + m^c) = m + m^c - 1 = 0,$$

sendo 0 o neutro da soma de números reais!

Finalmente, temos que

$$\mathbb{R} = \mathbb{R}^+ \cap \{0\} \cap \mathbb{R}^-,$$

onde $\mathbb{R}^-$ é o conjunto dos opostos dos números reais positivos.

Assim, dado um número real x não nulo é positivo, ou seu oposto é positivo. Portanto podemos estender a ordem dizendo que $x > y$ se $x - y$ é um real positivo. Associe este fato à relação de ordem vista anteriormente para os números inteiros, e racionais. Também, é fácil ver que o teorema de completude ainda continua válido para esta extensão dos números reais positivos.

Mais um detalhe a ser considerado é a identificação feita para cada representação decimal de um número real positivo cuja mantissa termina em uma sequência de noves com um decimal finito, cuja mantissa termina em uma sequência de zeros. Recuperamos esta identificação de maneira natural da forma

$$\text{se } x \text{ está identificado com } y \text{ então } -x \text{ é identificado com } -y.$$

Esta identificação não altera a ordem nem a completude, sendo totalmente compatível com as definições das operações.

4.2 A Não Enumerabilidade dos Números Reais

Lembrando do módulo III, a enumerabilidade de um conjunto é a capacidade de dispor os números do conjunto como uma "'lista", mais precisamente, como uma sequência, em correspondência com o conjunto dos número naturais. O conjunto dos números irracionais não tem essa propriedade. Em outras palavras, diferentemente dos racionais, a "ordem de infinitude" da quantidade dos números irracionais é "maior" que a dos números naturais. Concluímos daí que existem muito mais números irracionais do que racionais!

Usando a representação decimal dos números reais do intervalo $[0, 1]$, vamos mostrar, então, que o conjunto dos número reais é não enumerável. Esta demonstração é devida a Cantor.

Teorema 4.2 (Cantor)**.** *O conjunto* $(0, 1]$ *não é enumerável.*

Demonstração: Suponha que o conjunto dos números reais entre 0 e 1 é enumerável. Então existe um enumeração, que podemos escrever como um sequência $s_1, s_2, \ldots, s_p \ldots$. Vamos criar um número irracional x entre 0 e 1 que não está na lista. Faremos isso através de uma representação decimal, portanto, uma dízima não periódica, da seguinte forma: o número x tem representação decimal dada por $0, \ldots\ x_{-1}x_{-2}x_{-3}\ldots$, onde x_{-p} é escolhido dentro do conjunto $\{0, 1, \ldots, 9\}$ de modo que x_{-p} é diferente de $(s_p)_{-p}$, onde este último é o algarismo que aparece na casa decimal de ordem p do irracional s_p, o $p-$ésimo elemento da sequência. A escolha de cada x_p também deve atender a condição de não permitir que nenhum grupo de algarismos dentre os já escolhidos, $x_{-1}x_{-2}x_{-3}\ldots$, possa se tornar o gerador de uma dízima periódica. Desta forma obtemos uma dízima não periódica representando um único irracional que, no entanto, não pode constar na lista da enumeração. De fato, se $x = s_r$ para algum elemento da lista, então deveríamos ter $x_{-r} = (s_r)_{-r}$, o que não pode acontecer da forma que foi construido o número x. ■

Na introdução deste módulo mostramos que $\sqrt{2}$ não é um número racional. Também vimos, com uma demonstração similar, que o número $\sqrt{5}$ não é um número racional (veja o desafio 4). Vamos ver, em forma mais geral, como podemos mostrar quando um número racional é solução da equação $x^n = \frac{a}{b}$. Deixamos esta demonstração como o primeiro desafio desta seção!

Desafio!

Dado um número racional não nulo $\frac{a}{b}$ na sua forma irredutível e um número natural n, quais são os números racionais x, tais que $x^n = \frac{a}{b}$?

Clique aqui para ver a resposta.

Agora que sabemos como identificar números que não são racionais, que denominaremos de números irracionais, vamos mostrar que esses números e os números racionais estão “bem

distribuídos" na reta real. Isto na seguinte proposição.

Proposição 4.5. *Dados dois números reais x e y, $x > y$, então*

1. *existe $r \in \mathbb{Q}$ tal que $x > r > y$;*
2. *existe $i \in \mathbb{R} - \mathbb{Q}$ tal que $x > i > y$.*

Demonstração:

1. Como temos $x - y > 0$ então, pela propriedade arquimedeana, temos a existência de $n_0 \in \mathbb{N}$ tal que $n_0(x - y) > 1$, o que significa que $n_0 x - n_0 y > 1$. Como a diferença entre os números $n_0 y$ e $n_0 x$ é maior do que 1, então tem que existir um número inteiro k tal que $n_0 x > k \geq n_0 x - 1 > n_0 y$ ou, equivalentemente, $x > \frac{k}{n_0} \geq x - \frac{1}{n_0} > y$. Fazendo $r = \frac{k}{n_0}$, o primeiro item está demonstrado.

2. Dividimos a prova em várias alternativas:

1. se ambos os números x e y são irracionais, então podemos escrever $x > y + \frac{x-y}{2} > y$;
2. se x é irracional y é racional, pelo item 1 temos que $x > x - \frac{1}{n_0} > y$ para algum n_0 natural;
3. se x é racional y é irracional, temos que $x > y + \frac{1}{n_1} > y$, para algum n_1 natural;
4. se ambos são racionais, isto foi provado no módulo 3.

■

Note que a demonstração da existência do número racional r na proposição 4.5 mostra não só que existe um número irracional, senão um número enumerável desses números, correspondente a cada escolha de $n \geq n_0$. A mesma conclusão para os outros casos.

Temos então que existem pelo menos um número enumerável de números irracionais. Existem mais do que isso?

A seguinte proposição mostra que o conjunto dos números irracionais é de fato um conjunto não enumerável. Esta afirmação será mostrada a partir da proposição de Cantor 4.2. Denotaremos ao conjunto $\mathbb{R} - \mathbb{Q}$, dos números reais que não são racionais, por $\mathbb{I}$.

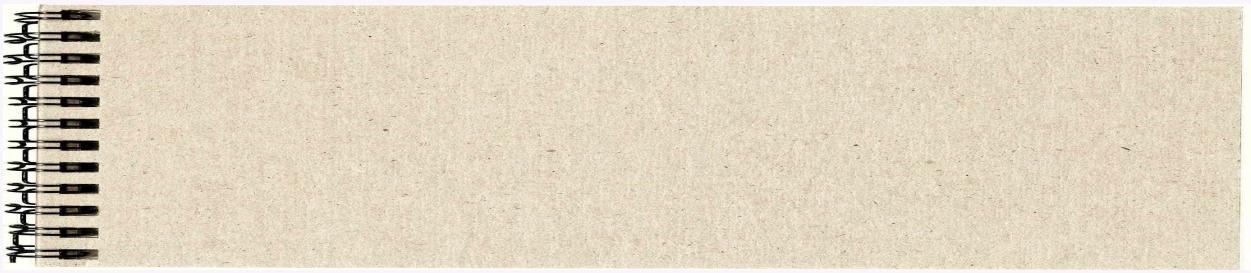
Proposição 4.6. *O conjunto $\mathbb{I}$ é não enumerável.*

Demonstração:

Temos que $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$. Assim, do fato que $\mathbb{Q}$ é enumerável, se $\mathbb{I}$ fosse enumerável, teríamos que $\mathbb{R}$ seria enumerável, por ser união de conjuntos enumeráveis. Porem, pelo teorema 4.2 isso é falso. ■

Desafio!

Mostre que a união de conjuntos enumeráveis é um conjunto enumerável.



Clique aqui para ver a resposta.

4.3 Os Números Irracionais

Introduzimos na seção anterior o conceito de número irracional. Vimos no módulo III que a soma e produto de números racionais sempre resulta em um número racional, isto é, estas operações são *fechadas* não conjunto $\mathbb{Q}$. Vamos mostrar que esta propriedade não é verdadeira para números irracionais, ou seja, as operações de adição e multiplicação não são fechadas em $\mathbb{I}$.

Exemplo 4.7. Por exemplo, $\sqrt{2}$ e $\sqrt{2}-1$ são números irracionais, mas $\sqrt{2}-1-\sqrt{2}$ tem como resultado -1, que não é um número irracional.
Da mesma maneira, o produto dos números irracionais $\sqrt{2}-1$ e $\sqrt{2}+1$ tem como resultado 1, que é um número racional.

Indo mais em diante com essa aritmética dos números irracionais, veremos na seguinte proposição um mecanismo para construir infinidade de números irracionais.

Proposição 4.7. *Seja r um número racional e i um número irracional, então $r+i$ é irracional.*

Demonstração: Suponha que $x = r + i$ seja um número racional. Então, sendo r um número racional, seu oposto $-r$ também o é. Como consequência $x - r = x + (-r)$ é um número racional, pois a adição é fechada em $\mathbb{Q}$. Concluindo que i é um número racional. Isto é uma contradição com a hipótese. ■

Exemplo 4.8. Seja n um número natural qualquer. Então, pela proposição 4.7, os números do conjunto $A = \{a = n + \sqrt{2},\ n \in \mathbb{N}\}$ são números irracionais. Como podemos estabelecer a correspondência $f : \mathbb{N} \to A$ tal que $f(n) = n + \sqrt{2}$ que é uma bijeção, então o conjunto A tem a mesma cardinalidade de $\mathbb{N}$.

Na próxima seção faremos uma classificação dos números irracionais pela propriedade de ser ou não raiz de um polinômio de coeficientes racionais.

4.3.1 Números reais algébricos e transcendentes

A teoria dos números algébricos foi criada na segunda metade do século XIX nos trabalhos dos matemáticos Ernest Kummer (1810-1893), Richard Dedekind (1831-1916) e Leopold Kronecker (1823-1891). Essa teoria teve suas origens quando o matemático alemão Carl F. Gauss (1777-1855) estendeu a idéia de número inteiro definindo o anel dos inteiros algébricos gaussianos, $Z[i]$, e posteriormente na tentativa de se demonstrar o último teorema de Fermat.

Por outro lado, a origen da "transcendência" dos números se remonta aos gregos, tentando resolver problemas geométricos como a duplicação do cubo, trissecção do ângulo e a quadratura do círculo, problemas irresolúveis com régua e compasso. Em 1844 Hilbert propôs o chamado sétimo problema de Hilbert, cuja solução foi obtida em 1934 pelo matemático ucraniano Israil Gelfand (1913-2009) e Theodor Schneider (1911-1988). Em 1874 Cantor demonstrou a existência de números transcendentes, provando que os números algébricos tem a mesma cardinalidade do conjunto dos números naturais. Depois de ter demonstrado que o conjunto dos números reais não é enumerável, a conclusão foi que existem "muitos mais" números que não são algébricos. Em 1844 o matemático francés Joseph Liouville (1809-1882) construiu uns números transcendentes que levam seu nome. Em 1873 Charles Hermite (1822-1901) conseguiu demonstrar que o número de Euler (mais conhecido como número e) é transcendente. Finalmente, em 1882 o matemático alemão Carl Lindemann (1852-1939) mostrou que o número π é transcendente resolvendo um antigo problema dos gregos sobre a quadratura do círculo.

Desafio!

Depois de todas essas história com nomes de matemáticos “transcendentes”, o desafio é você ir nos links colocados acima e fazer um pequeno resumo da vida de cada um deles, relacionado com o tópico de número algébrico e transcendente. No máximo de cinco linhas para cada matemático. A fonte da University of St Andrews, da Escócia é uma das melhores do mundo em biografias da história da Matemática. A página está em inglês...esse é, então, o GRANDE desafio!

Coloque a redação exercício número 1 da lista do caderno de execícios do módulo IV 

.

Vamos começar com a definição de número algébrico.

Definição 4.11. *Um número real x é dito algébrico, se existir $n \in \mathbb{N}$ e números racionais $r_0, r_1, r_2, \ldots, r_{n-1}$, tais que*

$$x^n + r_{n-1}x^{n-1} + \ldots + r_2x^2 + r_1x + r_0 = 0.$$

Em outras palavras, um número real é algébrico se for raiz de algum polinômio de coeficientes racionais.

Exemplo 4.9. Seja $n \in \mathbb{N}$ um número natural que não é um quadrado perfeito, isto é, não existe $a \in \mathbb{N}$ tal que $a^2 = n$, então $\sqrt{n}$ é um número irracional algébrico.

A tarefa de descobrir se um número real é algébrico pode ir de simples a muito complicada. Vamos ver uma proposição que mostra que os números algébricos são “pelo menos” um conjunto enumerável.

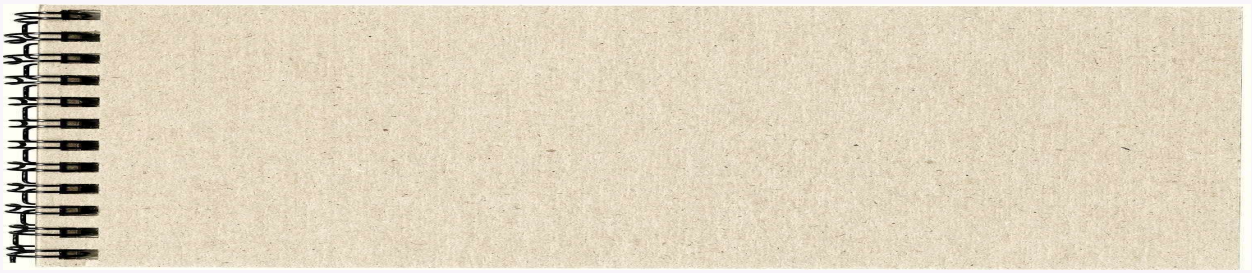
Proposição 4.8. *Todo número racional é um número algébrico.*

Demonstração: Seja $r \in \mathbb{Q}$. Então, considerando o polinômio $p(x) = x - r$, temos que r é raiz do polinômio. ■

Exemplo 4.10. Outro exemplo de um número irracional algébrico é o conhecido como **número de ouro** $\frac{1+\sqrt{5}}{2}$, raiz do polinômio $x^2 - x - 1$.

Desafio!

Mostre que os números $\sqrt[5]{3}$ e $\sqrt{2}$ são algébricos.



Clique aqui para ver a resposta.

Exemplo 4.11. Seja $x = \sqrt{2} + \sqrt{3}$. Temos que

$$\begin{aligned} x^2 &= \left(\sqrt{2} + \sqrt{3}^2\right) \\ &= 5 + 2\sqrt{6} \end{aligned}$$

e também

$$\begin{aligned} x^4 &= (\sqrt{2} + \sqrt{3})^4 \\ &= (5 + 2\sqrt{6})^2 \\ &= 49 + 20\sqrt{6}. \end{aligned}$$

Portanto,

$$x^4 - 10x^2 + 1 = 49 + 20\sqrt{6} - 10(5 + 2\sqrt{6}) + 1 = 0,$$

o que prova que $x = \sqrt{2} + \sqrt{3}$ é um número algébrico

Observação 4.7. Pode-se provar que se a e b são números algébricos então a soma e o produto são números algébricos. Na realidade o conjunto dos números algébricos tem uma estrutura de corpo com essas operações.

Definição 4.12. *Um número que não é algébrico é definido como número real transcendente.*

Os mais famosos números transcendentes são o número π e o número e também denominado **número de Euler**, que você muito bem conhece dos cursos de cálculo.

Daremos a seguir uma ideia de porque os números π e e são números irracionais e transcendentes.

Como curiosidade, até o momento, ainda se desconhece se os números $\pi \cdot \mathrm{e}$ e $\pi \cdot \mathrm{e}$ são ou não transcendentes.

A prova da irracionalidade de π e e se baseia em uma afirmação demonstrada por Parks (1986) que, por sua vez é uma generalização da prova que Ivan Niven fez em 1947 da irracionalidade do número π.

Como leitura complementar no Moodle você pode encontrar o artigo original (de uma página) de Niven.

O enunciado envolve noções de cálculo, por isso achamos agradável de ser lida.

Teorema 4.3. *Seja f um função definida em $[0, c]$, contínua e positiva em $(0, c)$, tal que suas primitivas, definidas no mesmo intervalo, verificam a fórmula de recorrência $F' = f$ e $F^{n+1} = F^n$, onde F^n significa a derivada $n-$ésima da função F. Então c tem que ser um número irracional.*

Com esta afirmação resulta fácil ver que o número π é um número irracional:

A função $f(x) = \mathrm{sen}(x)$ é continua em $[0, \pi]$ e positiva em $(0, \pi)$ com sequência das primitivas de f verificando a recorrência $-\cos x, -\mathrm{sen}x, \cos x, \mathrm{sen}x, \ldots$, no intervalo $[0, \pi]$. Logo, pelo teorema 4.3, o extremo positivo tem que ser um número irracional.

A irracionalidade de e pode-se deduzir também do teorema 4.3, mostrando que se a é um número positivo diferente de 1 então, se $\ln a$ é um número racional, devemos ter a como um número irracional. Como temos que $\ln \mathrm{e} = 1$, que é um número racional, então e tem que ser um número irracional.

4.4 Outras construções do conjunto dos números reais

4.4.1 Os cortes de Dedekind

O método mais sutil para a construção dos números reais é devido a Richard Dedekind que em 1872 publicou o trabalho sobre um modelo de construção dos números reais. Para esta construção, se supõe os números inteiros e racionais já conhecidos. Assim, um corte de Dedekind é um conjunto C de números racionais tais que

1. se $x \in C$ e $y < x$, então $y \in C$;
2. $C \neq \emptyset$ e $\mathbb{Q} - C \neq \emptyset$;
3. C não possui máximo.

Observação 4.8. Note que a idéia de Dedekind é pensar um número real x como o ponto extremo direito de um intervalo infinito do tipo $(-\infty, x)$. Este intervalo é constituído exclusivamente por números racionais.

Neste modelo, os números reais são definidos como sendo o conjunto de cortes de Dedekind. A relação de ordem é feita comparando dois cortes C_1 e C_2: se $C_1 \subset C_2$ então $C_1 < C_2$. A adição também corresponde aos conjuntos soma dos cortes, $C_1 + C_2$. Assim definido, temos, por exemplo, que o neutro da adição no modelo de Dedekind é o intervalo $(-\infty, 0)$.

Já a multiplicação é um pouco mais complicada de definir, porém, uma vez que está todo definido, não é difícil verificar os axiomas de número real.

4.4.2 As sequências de Cauchy

O método de maior alcance para a construção dos números reais é devido, independentemente, a Charles Meray (1869, 1872) e Georg Cantor, matemático já mencionado neste módulo.

Mais uma vez, o processo construtivo se baseia na estrutura de corpo dos números racionais. Considera-se o conjunto $\mathcal{C}$ das sequências $\{x_n\}$ de números racionais que verificam

$$\lim_{\substack{n\to\infty \\ m\to\infty}} |x_n - x_m| = 0.$$

Tais sequências são chamadas de sequências de Cauchy.

Define-se uma relação de equivalência no conjunto $\mathcal{C}$, de forma que duas sequências de Cauchy x_n e y_n são equivalentes se

$$\lim_{n\to\infty} |x_n - y_n| = 0.$$

O conjunto dos números reais é assim, o conjunto quociente determinado por essa relação de equivalência no conjunto $\mathcal{C}$. Adição é definida através de representantes das classes como

$$[x_n] + [y_n] = [x_n + y_n],$$

demonstrando que esta definição não depende do representante escolhido. A mesma ideia segue a definição de produto.

Existe neste modelo um árduo trabalho na verificação dos axiomas de corpo ordenado e principalmente no axioma de completude. A vantagem é que as ideias do modelo podem ser usadas em um contexto mais geral, como é o dos **espaços métricos**  .

4.5 Unicidade do corpo dos números reais

O objetivo desta seção é mostrar em linhas gerais como é feita a prova da unicidade do corpo ordenado e completo dos números reais (aquela estrutura que verifica a axiomática da aritmética, da ordem e da completude)

Começamos a prova tomando um conjunto de reais construído em qualquer das formas expostas na seção 4.4. Atribuímos a cada x do conjunto uma representação decimal como explicamos a seguir:

- Seja a_0 o maior inteiro que é menor ou igual ao real a. Assim temos $0 \leq a_0 \leq a$.
- Determine o número inteiro a_1 o maior inteiro tal que $a_0 + \frac{a_1}{10} \leq a$.
- Determine o número inteiro a_2 o maior inteiro tal que $a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} \leq a$.
- Continuando, obtemos $a_0\ , a_1,\ a_2, \ldots,\ a_{n-1}$. Encontramos o inteiro a_n, o maior inteiro tal que

  $$a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_{n-1}}{10^{n-1}} + \frac{a_n}{10^n} \leq a$$

  com a_n no conjunto $\{0,\ 1,\ 2, \ldots,\ 9\}$.

Assim, cada x determina uma representação decimal $D = a_0, a_1 a_2 \ldots a_n \ldots$ decimal infinito.

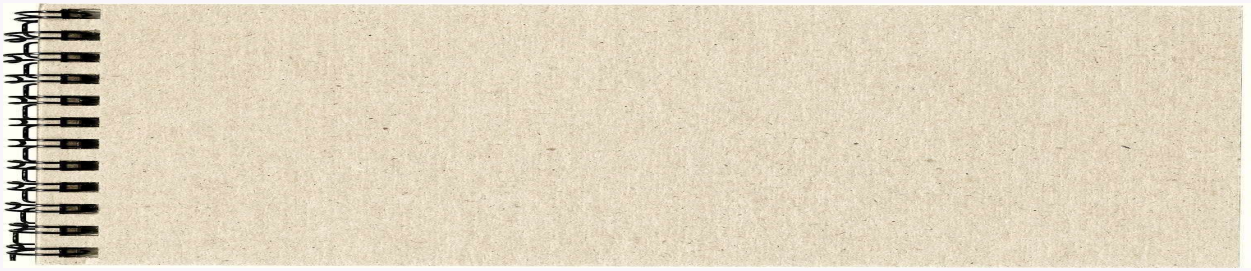
Gostaríamos de mostrar, então, que a função f entre o corpo dos reais e o conjunto das representações decimais que faz corresponder x com a representação decimal obtida na construção acima é bijetora, preservando as operações e a ordem.

Vamos demonstrar na seguinte proposição que f é de fato uma bijeção.

Suponha $y \neq x$, ou mais especificamente $y > x$. Então, pela propiedade arquimedeana, existe n tal que $y - x > \frac{1}{10^n}$.

Desafio!

Prove como exercício a afirmação: se $y > x$, então existe n tal que $y - x > \frac{1}{10^n}$. Escreva a demonstração no caderno.



Clique aqui para ver a resposta.

Assim entre x e y existe um intervalo de comprimento $\frac{1}{10^n}$, de modo que os primeiros n dígitos da representação decimal de y não podem ser os mesmos que as do x. Isto conclui que $f(x) \neq f(y)$.

Note que a forma de construir a imagem do número real x, não pode ser uma representação com uma sequência de infinita de dígitos noves. Com efeito, se x tem como imagem $a_0, a_1a_2 \ldots a_m \ldots 999 \ldots$ e r é um número racional tal que $r - x < \frac{1}{10^m}$ para m natural, então $x = r$, contrariando o fato de que o decimal correspondente a x termina em noves e não em zeros.

Para mostrar que f é sobrejetora, devemos mostrar que se $D = z, a_1a_2 \ldots$ é um decimal que não termina em noves então existe um número real x tal que $f(x) = D$. Nesta parte usamos a completude do modelo.

Considerando o conjunto A definido por

$$A = \{d_n = z + \tfrac{a_1}{10} + \ldots + \tfrac{a_1}{10^n}, n \in \mathbb{N}\},$$

temos que $z + 1$ é uma cota superior de A, portanto existe um número real $x = \sup A$. Verificamos facilmente que $f(x) = D$ seguindo a construção da imagem descrita acima.

Para completar a prova da unicidade, devemos mostrar que que f preserva a aritmética e a ordenação. Esta última decorre diretamente da definição. A preservação da estrutura de corpo pode levar algumas páginas que deixamos para a curiosidade do leitor.

Esta demonstração da unicidade nos fornece uma forma de encontrar os números racionais da sequência de truncamentos de um número irracional. Vejamos um exemplo.

Exemplo 4.12. Sabendo-se que uma aproximação para $\sqrt{2}$ com quatro casas decimais é dada por $1,4142$, então os quatro primeiros elementos da sequência de truncamentos é

$$\{x_1 = 1,\ x_2 = \frac{14}{10},\ x_3\frac{141}{100},\ x_4 = \frac{1414}{1.000},\ \frac{14142}{10.000}\cdots\}$$

e, além disso, temos

$$0 < \sqrt{2} - x_i < \frac{1}{10^i} \quad \text{para } i = 1, 2, 3, 4.$$

Note que, do fato que existe um número racional r tal que

$$r - \sqrt{2} < \frac{1}{10^n} \quad \text{para algum } n \in \mathbb{N},$$

então podemos procurar aproximar o número $\sqrt{2}$ usando esta afirmação. Revisemos o algoritmo para as duas primeiras casas decimais de $\sqrt{2}$.

1. Encontre o maior número inteiro tal que $z_1^2 < 2$ e o menor inteiro tal que $z_2^2 > 2$. Temos que $z_1 = 1$ e $z_1 = 2$;

2. Agora, deve existir algum $n \in \mathbb{N}$ tal que $r_1 + \frac{n}{10} < \sqrt{2}$ e $r_2 - \frac{n}{10} > \sqrt{2}$. Sabendo que $r_1 = 1, x_1$, temos $n = 1$. Testamos com $1 + \frac{1}{10}$ cujo quadrado é

   $$\left(1 + \tfrac{1}{10}\right)^2 = 1^2 + 2 \cdot \tfrac{1}{10} + \left(\tfrac{1}{10}\right)^2 = \frac{121}{100}.$$

   Como $1,21 < 2$, podemos testar com $1,2$, cujo quadrado é $1,44$. Testando com $1,5$, notamos que $(1,5)^2 = 2,25$ que excede 2. Assim, o maior número racional menor que $\sqrt{2}$ e dista menos de $\frac{1}{10}$ é, de fato, $1,4$. Além disso, temos $1,4 < \sqrt{2} < 1,5$, o que nos confirma a informação que obtivemos teoricamente.

3. Repetindo o processo temos que $(1,41)^2 = 1,9881$ e que $(1,42)^2 = 2,0164$. Portanto, neste caso, temos que $1,41 < \sqrt{2} < 1,42$.

Você já pensou se pudéssemos fazer esse algoritmo de uma forma mais sistemática para encontrar muitas casas decimais de $\sqrt{2}$?

Tomemos a sequência definida por recorrência (veja a definição de sequência definida por recorrência no módulo I, que define a $\sqrt{2}$, dada pela fórmula

$$x_1 = 1, \qquad x_{n+1} = \frac{6x_n - x_n^3}{4}. \tag{4.22}$$

Claramente é uma sequência de números racionais. Pode-se provar que é crescente e limitada superiormente. Portanto, pelo teorema 4.1 tem um supremo que é $\sqrt{2}$.

Assim, usando a fórmula (4.22), obtemos rapidamente a seguintes aproximações:

$$\begin{aligned} x_1 &= 1; \\ x_2 &= 1,25; \\ x_3 &= 1,38671875; \\ x_4 &= 1,413416936993598937988281 25, \end{aligned}$$

notando a velocidade da sequência na aproximação da raiz quadrada de 2!

Uma sequência de truncamentos para a raiz quadrada de um número natural k é a seguinte:

$$x_1 = 1, \qquad x_{n+1} = \frac{3kx_n - x_n^3}{2k}. \tag{4.23}$$

Desafio!

Calcule o número $\sqrt{7}$ na sua calculadora. Quantas aproximações da sequência (4.23) se precisam para obter exatamente a mesma resposta que na calculadora?

Clique aqui para ver a resposta.

4.6 Respostas aos desafios do módulo 4

- Desafio da página 169.

  Vamos supor que existe d é um número racional que verifica $r^2 = 5$. Vamos tomar $d = \frac{a}{b}$ o representate irredutível com $b > 0$. Logo,

  $$\left(\tfrac{a}{b}\right)^2 = 5 \quad \text{ou equivalentemente} \quad a^2 = 5 \cdot b^2. \tag{4.24}$$

Deduzimos da segunda igualdade em (4.24) que $5 \mid a^2$. Portanto temos que $5 \mid a$. Assim temos

$$a = 5 \cdot k, \quad \text{para algum } k \text{ inteiro.} \tag{4.25}$$

Voltando à segunda igualdade em (4.24), vamos substituir a escrito como em (4.25), obtendo

$$\begin{array}{l} (5 \cdot k)^2 = 5 \cdot b^2 \quad \text{ou equivalentemente} \\ 5^2 \cdot k^2 = 5 \cdot b^2 \quad \text{e dividindo por 5 obtemos} \\ 5 \cdot k^2 = b^2. \end{array}$$

Esta última igualdade confirma que $5 \mid b^2$ e portanto $5 \mid b$. Ou seja, concluímos que o MDC(a, b) é pelo menos 5. Isto é uma contradição com o fato de que $\frac{a}{b}$ é uma fração irredutível.

A modo de se exercitar, refaça a prova para o número primo 7.

- Desafio da página 174. As cotas superiores do conjunto

$$A = \{x = \tfrac{1}{n},\ n \in \mathbb{N}\}.$$

são todos os números reais maiores ou iguais que 1 pois

$$\tfrac{1}{n} \leq 1 \quad \text{para todo} \quad n \in \mathbb{N}.$$

Por exemplo, $2;\ 100;\ 1,1$ são cotas superiores.

As cotas inferiores de A são todos os números menores ou iguais a 0 pois

$$0 < \tfrac{1}{n} \leq 1 \quad \text{para todo} \quad n \in \mathbb{N}.$$

Este conjunto tem supremo que é o número 1, pois é a menor das cotas superiores e como ínfimo o número 0, que é a maior das cotas inferiores. Tem como máximo o número 1, pois é supremo e pertence ao conjunto A. Não possui mínimo, pois o candidato seria 0, que é o ínfimo, mas este número não pertence a A.

- Desafio da página 176.

$$\begin{array}{rcl} A + B & = & \{1+0, 1+1, 1+2, -1+0, -1+1, -1+2, 3+0, 3+1, 3+2\} \\ & = & \{1, 2, -1, 0, 3, 4, 5\} \end{array}$$

- Desafio da página 181. O número

$$b = 5,2231\overbrace{0}^{1 \text{ zero}}2\overbrace{00}^{2 \text{ zeros}}2\overbrace{000}^{3 \text{ zeros}}\ldots 2\overbrace{0\ldots0}^{n \text{ zeros}}2\ldots$$

é um número que, a partir da quarta casa decimal, repete a seguinte sequência: o número 2 seguido de n zeros para cada $n \in \mathbb{N}$.

- Desafio da página 183.

  Temos que $x(10) = 2.236067977$.

- Desafio da página 183.

  Para a raíz de 2 temos que a sequência de truncamentos até a posição 15 é

  $\{$1;1,4;1,41; 1,414; 1,4142; 1,41421; 1,414213; 1,4142135; 1,41421356; 1,414213562;

  1,4142135623; 1,41421356237; 1,414213562373; 1,4142135623730; 1,41421356237309$\}$

- Desafio da página 186.

  Por definição de ordem, temos que

  $$3 < 3,1 < 3,14 < 3,141 < \ldots,$$

  o que mostra que a sequência é estritamente crescente. Também temos que para qualquer n, $x(n) < 4$, o que mostra que o conjunto dos truncamentos do número pi é limitado superiormente.

- Desafio da página 191. A expressão $x^n = \frac{a}{b}$ é equivalente à expressão $b \cdot x^n = a$. Suponha que existe o número racional irredutível $\frac{c}{d}$ tal que

  $$\left(\frac{c}{d}\right)^n = \frac{a}{b},$$

  então

  $$\frac{c^n}{d^n} = \frac{a}{b},$$

  ou, equivalentemente,

  $$a \cdot c^n = d^n \cdot b.$$

  Logo, temos que c divide $a \cdot d^n$ e d divide $c^n \cdot b$. Uma vez que temos $\mathrm{MDC}(c,d) = 1$, devemos também ter que $\mathrm{MDC}(c,d^n) = 1$ e $\mathrm{MDC}(c^n,d) = 1$. Portanto, concluímos que c divide a e d divide b. Ou seja, se existirem números racionais tais que $x^n = \frac{a}{b}$, então devem ser fraçõoes cujos numeradores são divisores inteiros de a e os denominadores são divisores inteiros de b.

  Desafio da página 193. Suponha que A e B são conjuntos enumeráveis. Então existes enumerações f_1 e f_2 do conjunto dos números naturais em A e B, respectivamente. Considerando a função $\mathbb{N} \times \mathbb{N} \to A \cup B$ definida por

  $$g(m,n) = f_m(n), \text{ onde } m = 1, 2,$$

  é claramente uma função bijetora. Como vimos no módulo III, o conjunto $\mathbb{N} \times \mathbb{N}$ é enumerável, de onde o conjunto $A \cup B$ também o é.

- Desafio da página 196.

  O número $\sqrt{2}$ é algébrico porque é raíz do polinômio $x^2 - 2$. O número $\sqrt[5]{3}$ é algébrico pois é raíz do polinômio $x^5 - 3$.

- Desafio da página 200.

  Tendo $y > x$, temos que $r = \frac{1}{y-x} > 0$. Assim, existe o número real $q = \log_{10} r$. Como o conjunto dos números naturais não é limitado superiormente, então existe n_0 tal que $n_0 > q$. Portanto $10^{n_0} > \frac{1}{y-x}$ ou, equivalentemente, $y - x > 10^{n_0}$.

- Desafio da página 202.

  Usando a calculadora, temos que a aproximação dada é $\sqrt{7} = 2,64575131106459$. Usando a fórmula (4.23) obtemos

$$
\begin{aligned}
x_1 &= 1; \\
x_2 &= 1,\overline{428571}; \\
x_3 &= 1,934610579; \\
x_4 &= 2,384722867324352; \\
x_5 &= 2,608392301310890; \\
x_6 &= 2,644963750445851; \\
x_7 &= 2,645750959449806; \\
x_8 &= 2,645751311064520; \\
x_9 &= 2,645751311064590,
\end{aligned}
$$

  ou seja precisamos de 9 aproximações para chegar ao resultado da calculadora. Este exercício pode variar a resposta dependendo do poder da sua calculadora!

Referênci Bibliográfic

[1] ÁVILA, G., *Várias Faces da Matemática*, Tópicos para Licenciatura e Leitura Geral, Ed. Blucher, São Paulo, 2007.

[2] DOMINGUES, H. H., *Fundamentos de Aritmética*, Atual Editora, São Paulo, 1991.

[3] FIGUEIREDO, D. G. *Números irracionais e transcendentes*, SBM Coleção Fundamentos da Matemática Elementar, Rio de Janeiro, 1985.

[4] GOWERS, T., *Mathematics: A Very Short Introduction*, Oxford, 2002.

[5] HEFEZ, A., *Elementos de Aritmética*, Coleção Textos Universitários, SBM, Rio de Janeiro, 2005.

[6] MILIES, C. P. e COELHO, S. P., *Números: Uma Introdução à Matemática*, 3a edição, EDUSP, São Paulo, 2003.

[7] PARKS, A.E. *Pi, e and other irrational numbers*, The American Mathematical Monthly, 93, 722-723, (1986).

Prezado Aluno

Para melhor compreensão deste módulo pesquise e leia a bibliografia sugerida. Como leitura complementar sugerimos os seguintes textos:

[8] ALENCAR FILHO, E. *Teoria elementar dos números*. Nobel, São Paulo, 1992.

[9] Clark E.W., *Elementary Number Theory*, Lectures Notes, Department of Mathematics University of South Florida, 2003

[10] GRAÑA, M., JERÓNIMO G., PACETTI, A., *Los números: de los naturales a los complejos*, 1a ed., Buenos Aires: Ministerio de Educación de la Nación. Instituto Nacional de Educación Tecnológica, 2009.

[11] NIVEN, I.; ZUCKERMAN, H. S. *An introduction to the theory of numbers*. 3rd. Edition, John Wiley, New York, 1972.